DISEÑO E IMPLEMENTACIÓN DE UN MODELO Y PLAN DE RECUPERACIÓN PARA LA GERENCIA DE TI, EN EL PROCESO DE RESPALDO DE INFORMACIÓN EN EMPRESAS DEL SECTOR QUÍMICO.

AUTOR

RICARDO RAFAEL MÁRCELES RUIZ

TRABAJO DE GRADO PARA OPTAR POR EL TÍTULO DE

MAGISTER EN GOBIERNO DE TECNOLOGÍA INFORMÁTICA

DIRECTOR

OSCAR JOSÉ DE LA OSSA VELEZ

UNIVERSIDAD DEL NORTE

FACULTAD DE INGENIERÍA DE SISTEMAS

BARRANQUILLA

2017

Contenido

Índice de imágenes

Índice de tablas

Índice de gráficos

Nota Aclaratoria

Este documento se prepara con el único propósito que haga parte de los requisitos para obtener el grado de Maestría en Gobierno de TI por parte de su autor, por lo que tiene fines meramente académicos y de consulta o revisión por parte de los jurados, profesores, estudiantes y asesores que de alguna forma deban consultarlo y/o comentarlo como aporte a dicho fin.

En el evento que alguno de sus lectores asocie su contenido con alguna empresa en particular, será producto de su libre entender, por lo que su autor no se hace responsable de ello.

1. Introducción

La mejor manera de preservar los bienes de la Empresa es garantizar la integridad de los trabajadores, no deteriorar el medio ambiente y no afectar la comunidad vecina, es actuar en nuestros puestos de trabajo con responsabilidad y cumplir los procedimientos y normas establecidos por la Empresa, de manera que se reduzca a un mínimo la posibilidad de ocurrencia de un accidente mayor. De cualquier manera, es necesario estar preparados para afrontar las emergencias que se deriven de un evento que pueda afectar la normal operación de la organización, mediante la formulación de planes y procedimientos para controlarlas y manteniendo a la Organización, las Brigadas y todo el personal debidamente preparados y entrenados.

Debe anotarse que en toda actividad industrial pueden ocurrir accidentes, a pesar de los múltiples esfuerzos que se hacen constantemente para prevenirlos. Con alguna frecuencia estos accidentes dan lugar a lesiones personales y daños en las instalaciones, en una extensión que depende del potencial que encierran estos eventos. En la industria química han ocurrido pérdidas severas en términos humanos y económicos. Pero también es cierto que en la mayoría de los incidentes, se han evitado pérdidas por la acción efectiva y oportuna de las Brigadas de Emergencia, y por la existencia de planes o procedimientos para controlarlas.

La historia de **"la organización"**[1] se inicia en septiembre de 1967, cuando el Consejo Nacional de Política Económica aprobó el proyecto destinado a la elaboración de productos químicos y Fertilizantes Compuestos, como culminación del estudio de factibilidad presentado en 1965 por el Fondo de Estudios Petroquímicos.

En diciembre del mismo año se elevó a escritura pública la constitución de **"la organización"**, como sociedad de responsabilidad limitada, en 1968 ingresó como accionista la firma licenciadora del proceso Stamicarbon de Holanda, se modificó la razón social y se cambió la forma jurídica de la empresa.

En 1972 se concluyó el montaje de las plantas, procediendo a la puesta en marcha y normalización de operaciones. Y en 1973, se iniciaron las actividades comerciales.

En 1985 se transformó la compañía acogiéndose a las ventajas que otorga el Acuerdo de Cartagena y posteriormente se abrió una sucursal en un país vecino, aprovechando las ventajas de ser considerada como nacional en el mismo.

En 1990 se creó una compañía filial la cual presta un servicio de carga dedicado a Colombia desde el Norte de Europa, Escandinavia, El Reino Unido, España, Estados Unidos y África Occidental. Esta exitosa Empresa es el resultado de la asociación de **"la organización"**, con un grupo naviero de Dinamarca.

En 2002 se adquirió la operación de una empresa de fertilizantes en Colombia, la cual pasó a llamarse **"la organización fertilizante"**[2], se dedica a la producción y comercialización de fertilizantes simples y mezclados. Tiene su sede social en Bogotá y la planta de producción de mezclas en Buenaventura.

En 2003 se creó la empresa **"la organización International Ltda."**[3], esta Empresa con sede

[1] Nombre cambiado a solicitud de la empresa para mantener confidencialidad de su información.
[2] Nombre cambiado a solicitud de la empresa para mantener confidencialidad de su información.
[3] Nombre cambiado a solicitud de la empresa para mantener confidencialidad de su información.

en las Islas Vírgenes Británicas, tiene como objetivo el de realizar operaciones logísticas y comerciales tanto con **la organización** como con terceros y el de agilizar la gestión documentaria de las importaciones de **la organización**.

El 21 de diciembre de 2006 el socio compró las acciones y después de esta transacción la participación del socio en **"la organización"** es del 100%.

1.1. Formulación del problema

1.1.1. Antecedentes

"La organización" tiene más de 45 años de trayectoria en Colombia, es líder junto con su filial **la organización fertilizante** en el mercado colombiano con una participación de más del 35% en las ventas de fertilizantes y productos químicos.

La organización tiene distribuida sus fuerzas de producción en sus complejos industriales ubicados a lo largo y ancho de la geografía colombiana generando cerca de 800 empleos directos y más de 1.300 oportunidades de trabajo a través de empresas prestadoras de servicios, actualmente tiene sus servicios informáticos centralizados donde se le presta servicio a más de 1.000 usuarios.

Durante el ejercicio de auditoría externa en el año 2016, la revisoría fiscal detectó que si bien **la organización** cuenta con un Datacenter en óptimas condiciones y unas tareas programadas de Backups[4], no se tiene un procedimiento establecido y documentado para llevar a cabo las actividades correspondientes para la recuperación ante emergencias; de igual manera no se tiene el procedimiento oficial para la puesta en marcha de la operación en sitios alternos de trabajo si llegase a suceder un evento que ponga en juego la continuidad del negocio ante una eventualidad.

Es importante tener en cuenta que, para **la organización**, la gerencia de Automatización Informática y Telecomunicaciones (**AIT**) así como sus servicios son habilitadores y apoyan a la operación como se muestra en la imagen a continuación:

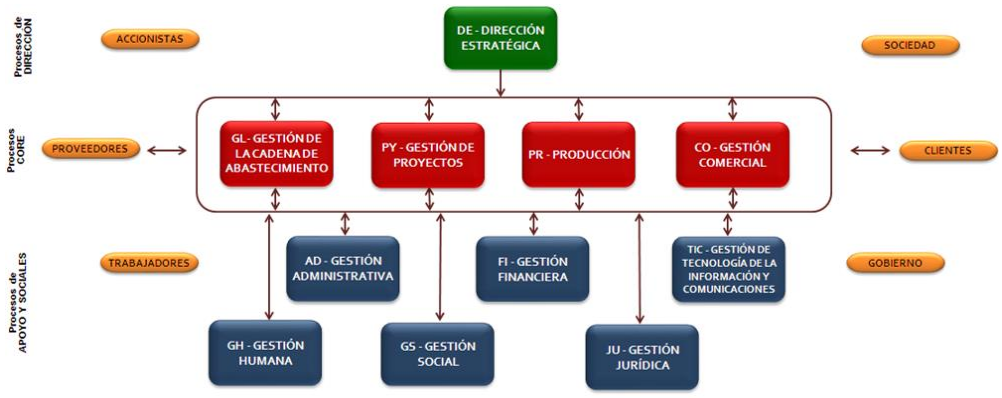

Imagen 1 - Red de procesos de la Organización[5]

Históricamente no se han presentado inconvenientes o eventos catastróficos en la organización que hayan puesto en peligro la continuidad de la operación tecnológica; sin

[4] Respaldo de información en cintas y/o medio magnético
[5] Red procesos PHVA de la organización, fuente: http://www.laorganización.com.co/intranet

embargo, la gerencia AIT responsable de estas actividades no cuenta con un proceso documentado, probado y formalizado que pueda ser activado o consultado al momento de sufrir algún tipo de incidente mayor.

A nivel mundial y en el sector de negocio en el que se desenvuelve la organización, se han registrado varios incidentes que han puesto en vilo la continuidad de las empresas involucradas, los casos que más se traen a colación al momento de realizar simulacros son:

- **West Fertilizer Company**: El 17 de abril de 2013 en la ciudad de West, Texas, ocurrió una explosión en la planta de almacenamiento y distribución de fertilizantes de la compañía, donde se almacenaba nitrato de amonio, a 29 kilómetros (18 millas) al norte de la ciudad de Waco, cuando el personal de servicios de emergencia estaba respondiendo a un incendio en la instalación, 15 personas fallecieron, más de 160 resultaron heridos, y más de 150 edificios resultaron con daños leves o destruidos.[6]

- **Explosiones en Tianji de 2015**: El incidente ocurrió en el Distrito de Binhai, que corresponde a la zona portuaria de la ciudad de Tianjin. En la noche del miércoles 12 de agosto, comenzó un incendio en algunos contenedores del puerto, que causó dos gigantescas explosiones equivalentes al estallido de 21 toneladas de TNT. La primera ocurrió a las 23:40 (hora local). Las explosiones pudieron ser percibidas en un radio de 10 kilómetros, ocasionando graves daños hasta a 2 km a la redonda.

  Dentro de las causas se concluyó que el desastre fue causado por el incendio de materiales peligrosos, inapropiadamente o ilegalmente almacenados en el lugar. El primer incendio comenzó en un contenedor por la auto-ignición de nitrocelulosa, debido a la vaporización del elemento humectante a causa del clima cálido. El incendio se extendió, encendiendo otros químicos, incluyendo nitrato de amonio. [7]

2. Planteamiento del problema

2.1. Justificación

Debido a la sensibilidad de los datos y cantidad de información que se maneja al interior de la empresa durante su día a día, es imperativo definir y proporciona un marco administrativo para coordinar todas las actividades de respuesta operativa; esta actividad conllevará a obtener los siguientes beneficios:

a. Asegura la Continuidad del Negocio.
b. Proteger al negocio de fallas generales en los servicios informáticos.
c. Minimizar los riesgos generados por la falta de servicios.
d. Garantizar el acceso a la información clasificada como relevante definida por los líderes de negocio.
e. Mantener la disponibilidad de los recursos informáticos.
f. Minimizar la toma de decisiones confusas o erradas al presentarse algún desastre o incidente que demande activar los planes de continuidad.
g. Tener capacidad de recuperación exitosa.

[6] Fuente: https://es.wikipedia.org/wiki/Explosión_de_la_West_Fertilizer_Company
[7] Fuente: https://es.wikipedia.org/wiki/Explosiones_en_Tianjin_de_2015

3. Objetivos

Con el fin de respaldar el objetivo principal en nuestro mapa estratégico en el cual se busca "*Optimizar, mantener y mejorar la disponibilidad, confiabilidad, calidad, seguridad y continuidad de los servicios de TIC en* ***la organización*** *y filiales*" se definen los siguientes objetivos para este proyecto a cumplir en el presente documento:

- Diseñar un modelo para la elaboración del plan de continuidad y recuperación de incidentes para la gerencia AIT ante situaciones de emergencia.

- Diseñar e implementar un plan de continuidad para el proceso de respaldo de información para **la organización** y sus filiales.

4. Plan desarrollo trabajo de grado

El desarrollo del trabajo de grado se resume en 4 grandes etapas:

a) Revisión caso de estudio: Esta etapa comprende las actividades de Introducción, Formulación del problema, antecedentes, planteamiento del problema, justificación y objetivos.

b) Diseño del modelo propuesto: Esta etapa comprende el desarrollo del marco conceptual, definición de las metodologías a utilizar para el desarrollo del trabajo de grado (Octave y CoBit 5) así como la definición del modelo a implementar.

c) Guía de implementación: Esta etapa comprende el desarrollo del modelo metodológico, la explicación de los documentos a utilizar y la finalidad de los mismos en la ejecución del desarrollo del trabajo de grado.

d) Implementación del modelo propuesto: Esta etapa llevará a cabo la ejecución de lo explicado en la guía de implementación, de manera que se pueda evidenciar la aplicación de la teoría consultada en un caso práctico de negocio.

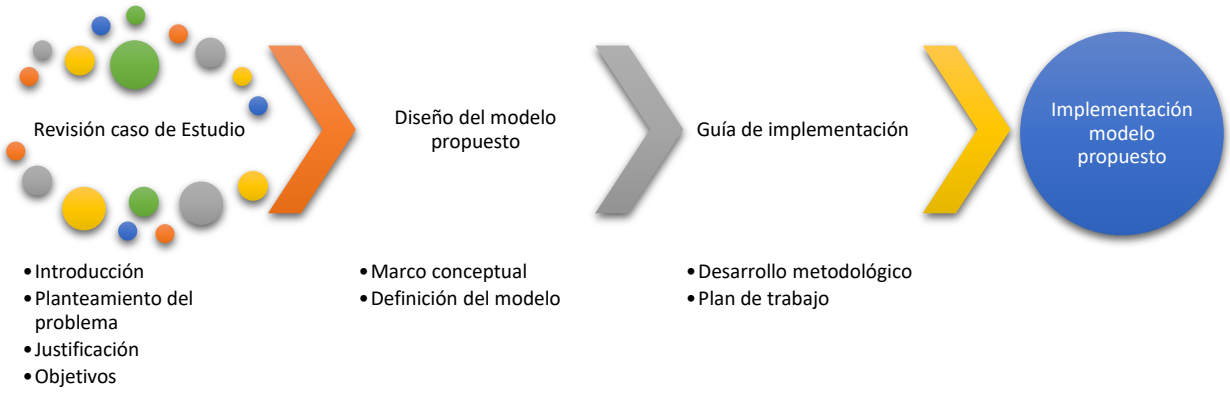

Imagen 2 - Plan desarrollo trabajo de grado

Teniendo en cuenta lo anterior, procederemos al desarrollo de cada uno de sus componentes para obtener un caso de estudio en el cual se pueda realizar una propuesta de valor para la organización esto con la finalidad de dar cumplimiento a los objetivos del presente trabajo de grado.

5. Marco Conceptual

Para realizar el ejercicio planeado, se utilizará los siguientes marcos referenciales:

5.1. Octave Allegro

Es una metodología para identificar y evaluar los riesgos de seguridad de la información, enfocado para ayudar a una organización a:

- Desarrollar criterios cualitativos de evaluación del riesgo que describe la tolerancia al riesgo operacional de la organización.
- Identificar activos que son importantes para la misión de la organización.
- Identificar vulnerabilidades y amenazas a esos activos.
- Determinar y evaluar las posibles consecuencias para la organización si materializan las amenazas.

"*El marco conceptual que formó la base original del enfoque OCTAVE fue publicado por el Instituto de Ingeniería de Software (SEI) de la Universidad Carnegie Mellon en 1999 [Alberts 1999]. Trabajando con el Centro de Investigación de Tecnología Telemedicina y Avanzada (TATRC), la SEI desarrolló el método OCTAVE para abordar los desafíos de cumplimiento de la seguridad Departamento de Defensa de los Estados Unidos (DoD) al abordar las disposiciones de la Portabilidad del Seguro Médico Y la Ley de responsabilidad (HIPAA) por la privacidad y seguridad de la salud personal."*[8]

Actualmente existen tres metodologías distintivas de OCTAVE disponible para uso público: OCTAVE, OCTAVE-S, y OCTAVE Allegro; cada método OCTAVE tiene amplia aplicabilidad, y los usuarios de estos métodos pueden seleccionar el enfoque que mejor se adapte a sus necesidades particulares. OCTAVE Allegro no pretende suplantar las metodologías anteriores pues es una variante que proporciona un proceso simplificado centrado en los activos de información que utilizaremos en el ejercicio a desarrollar para este trabajo de grado.

Con esta metodología podremos desarrollar una evaluación amplia del entorno de riesgo operacional de una organización buscando obtener resultados más robustos sin la necesidad de tener un amplio conocimiento de la evaluación de riesgos.

"*Este enfoque difiere de los anteriores de OCTAVE, centrándose principalmente en los activos de información, cómo se usan, donde se almacenan, transportan y procesan, y cómo son expuestos a amenazas, vulnerabilidades e interrupciones*"[9].

Al igual que los otros métodos, OCTAVE Allegro se puede realizar en workshops con equipos de trabajo conformados por personal mixto el cual puede estar integrado por personas de las áreas de negocio así como de AIT, esto con el fin de lograr identificar de una manera óptima las diferentes unidades de negocio y/o servicios vitales para la organización y que se consideren como neurálgicas para la continuidad del negocio ante una eventualidad.

[8] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, página 16
[9] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, página 16

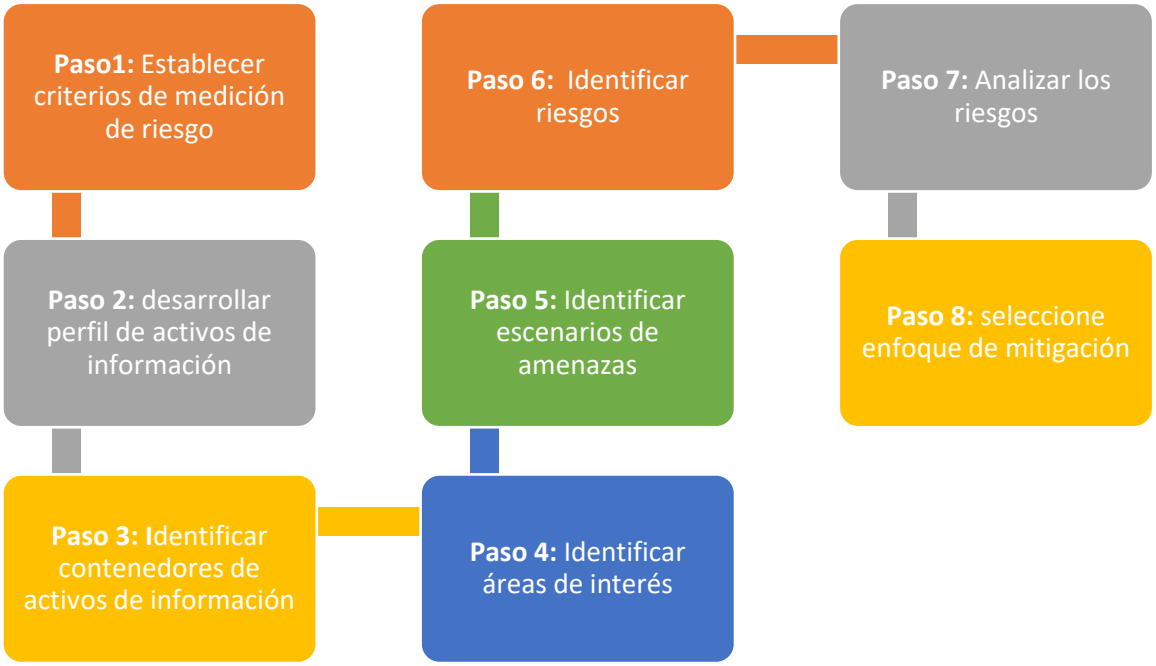

Imagen 3 - Pasos Metodología Octave[10]

Para el ejercicio a llevar a cabo, procederemos a trabajar con el **Paso 1** "**Establecer los criterios de la medición del riesgo**", **Paso 2** "**Desarrollar un perfil para el activo de información**" y **Paso 3**"**Identificar los contenedores de los activos de información**", los cuales serán descritos más adelante.

5.2. CoBit 5

Es un marco referencial que ayuda a las organizaciones a crear un valor óptimo a partir de la TI, al mantener un equilibrio entre la realización de beneficios y la optimización de los niveles de riesgo y utilización de los recursos, una descripción más exacta puede ser consultada en "Cobit5 Enabling - Spanish" como se enuncia a continuación:

"COBIT 5 incluye un modelo de referencia de procesos que define y describe en detalle varios procesos de gobierno y de gestión. Esto proporciona un modelo de referencia de procesos que representa todos los procesos encontrados normalmente en una empresa respecto a las actividades de IT, ofreciendo un modelo de referencia común entendible para gerentes de operativa TI y de negocio. El modelo de procesos propuesto es completo, exhaustivo, pero no es el único modelo posible. Cada empresa debe definir su propio conjunto de procesos, teniendo en cuenta su situación específica.

La incorporación de un modelo operacional y un lenguaje común a todas las partes de la empresa involucradas en actividades de TI es uno de los pasos más importantes y críticos hacia el buen gobierno. Esto también proporciona un marco para medir y supervisar el desempeño IT, comunicar con proveedores de servicio e integrar las mejores prácticas de gestión."[11]

"COBIT 5 permite que las tecnologías de la información y relacionadas se gobiernen y

[10] OCTAVE Allegro Roadmap
[11] ISACA, COBIT® 5: Enabling - Spanish, 2012, página 24

administren de una manera holística a nivel de toda la Organización, incluyendo el alcance completo de todas las áreas de responsabilidad funcionales y de negocios, considerando los intereses relacionados con la TI de las partes interesadas internas y externas"[12].

Los principios y habilitadores de COBIT 5 son genéricos y útiles para las organizaciones de cualquier tamaño, bien sean comerciales, sin fines de lucro o en el sector público; los dominios que podemos encontrar en CoBit 5 son los siguientes:

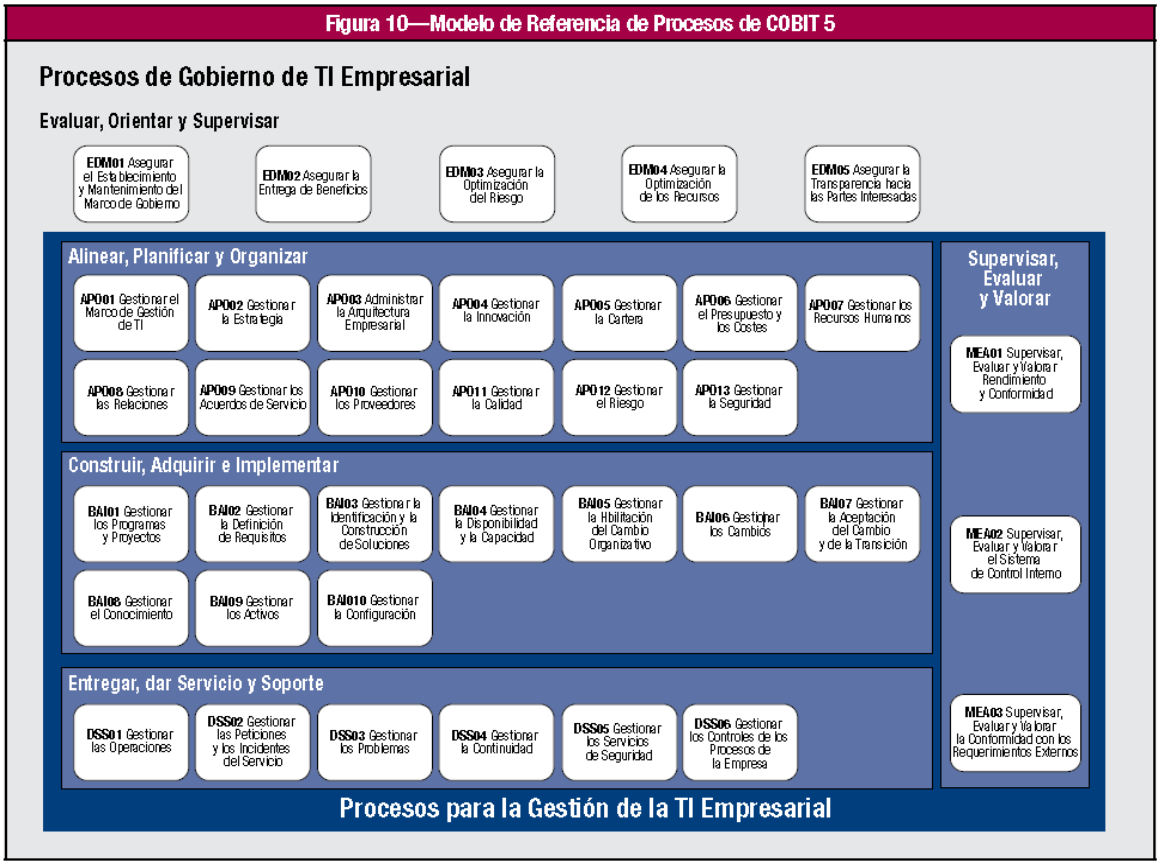

Imagen 4 - Modelo de referencia procesos de CoBit 5[13]

Para el ejercicio a realizar, procederemos a utilizar los dominios **APO12 "Gestionar el riesgo"**, **BAI01 "Gestión de programas y proyectos"** y **DSS04 "Gestionar la continuidad"**, los cuales serán descritos más adelante.

6. Definición del modelo

Teniendo en cuenta el planteamiento del problema y la necesidad presentada por la organización se propone crear el siguiente modelo de continuidad operativa para la gestión de incidentes:

[12] https://www.isaca.org/COBIT
[13] Modelo de Referencia de Procesos de COBIT 5

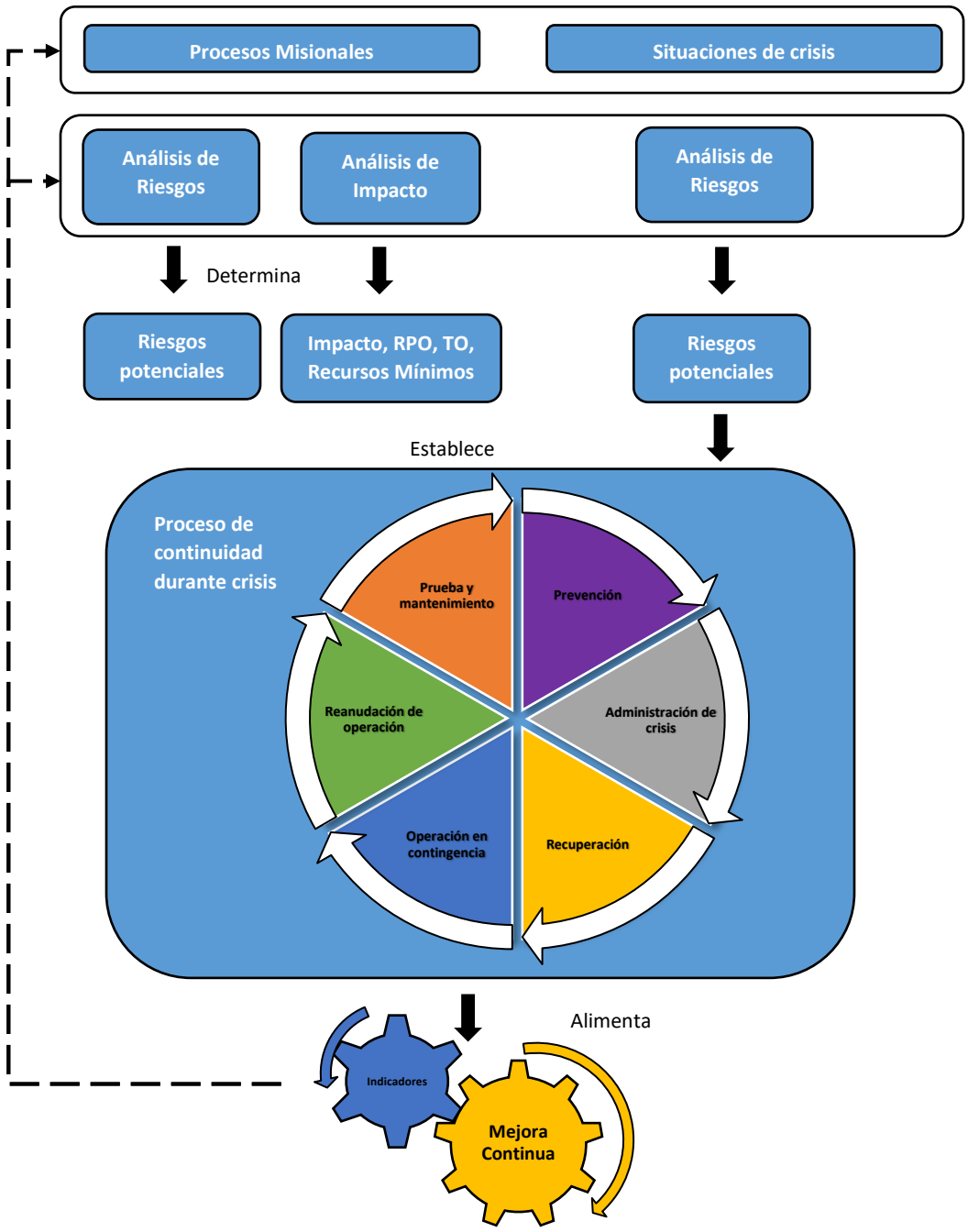

Imagen 5 - Modelo gestión continuidad operativa propuesto

6.1. Procesos misionales

Se evidencia que los procesos misionales de la organización son apoyados por los objetivos estratégicos de la gerencia de TI, basado en la metodología de BSC de la siguiente manera:

- **Financiero**
    - **F1:** Optimizar costos en la prestación de los servicios de TIC.

- **Procesos Internos**

    - **PI1:** Mantener y mejorar la disponibilidad, confiabilidad, calidad, seguridad y continuidad de los servicios de TIC

    - **PI2:** Entregar Soluciones de TIC que apoyen la estrategia

    - **PI3:** Mantener y fortalecer los procesos Internos

- **Aprendizaje y crecimiento personal**

    - **A1:** Fortalecer el uso de los recursos TIC

6.2. Análisis de riesgo y análisis de impacto

El modelo propuesto busca que los análisis de riesgos e impacto para los activos de información importantes en el proceso seleccionado, sean identificados con los pasos de Octave 1, 2 y 3 los cuales serán explicados más adelante.

Llevando a cabo este ejercicio, es posible entonces poder determinar el equipo a integrar y pasos a seguir durante una situación de crisis para mantener la continuidad operativa de la organización.

Para tener una adecuada valoración de riesgos y análisis de impacto, es necesario en primera instancia realizar un diagnóstico de la organización, esto con el fin de saber en el proceso de respaldo de información aquellos activos de información críticos para la organización y para la gerencia de TI, el contenedor de dicho activo, así como la "*hoja de vida*" del mismo.

6.3. Riesgo Potencial

Luego de levantar la información y llevar a cabo el análisis de riesgo e impacto, se determinará el riesgo potencial que deberá tratar la organización y las posibles vías de tratamiento, con el fin de tomar acciones preventivas con el área responsable de la gerencia AIT.

6.4. Proceso de continuidad durante crisis

Una vez llevada a cabo la ejecución de los análisis de riesgos y análisis de impacto de los activos de información de la organización, y teniendo en cuenta los resultados de los mismos en el momento que se detecta la emergencia, se determina si es necesario o no activar el proceso de continuidad operativa, éste se desglosa de la siguiente manera:

6.4.1.Prevención

Se definirá la estructura mediante la cual se dará tratamiento, esta información se encuentra a detalle en el **numeral 7.1** del presente documento, este numeral describe como se integrará el equipo multidisciplinario en la gerencia en aras de obtener un manejo adecuado de la situación de emergencia.

6.4.2.Administración de crisis

Se definirá la estructura mediante la cual se dará tratamiento a la crisis, esta información se encuentra a detalle en el **numeral 7.2** del presente documento, este numeral describe el paso a paso de cómo actuará la gerencia en el momento de crisis y los roles que desempeñarán los equipos de trabajo definidos en la fase de prevención.

6.4.3.Recuperación

Se definirán los tiempos máximos de tolerancia para la organización respecto a fallos generados debido a la situación de crisis, esta información puede ser consultada en el **numeral 7.3**.

6.4.4.Operación en contingencia

Se definen los roles y responsables que intervendrán en las diferentes actividades para la puesta en marcha de la operación mientras se restablece la normal operación.

6.4.5.Reanudación de operación

Se menciona el script o paso a paso que tendrá la gerencia y el área de infraestructura para iniciar operaciones luego de haber realizado los pasos anteriores de manera exitosa.

6.4.6.Prueba y mantenimiento

Teniendo en cuenta las lecciones aprendidas durante la etapa de crisis, se define un nuevo plan de pruebas y mantenimiento en caso de ser necesario, el detalle de estas actividades puede ser consultado en el **numeral 7.6** del presente documento.

6.4.7.Indicadores

Los indicadores de la gerencia serán actualizados y se definirán planes operativos con mediciones mensuales según lo considere el gerente del área, éstos serán tenidos en cuenta para la consecución de los objetivos corporativos a través de la ejecución de objetivos estratégicos por parte de la gerencia.

6.4.8.Mejora continua

Hace referencia a la medición de los planes operativos definidos en la gerencia y que son responsables de ejecutarlos todos y cada uno de los integrantes de la misma.

7. Proceso de continuidad operativa en crisis

Se define el siguiente proceso de continuidad para ser implementado en la organización, el cual se detalla a continuación:

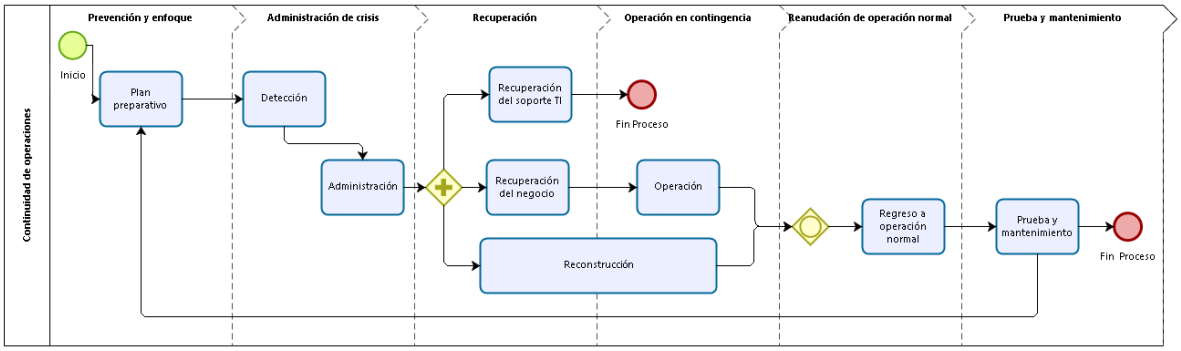

Imagen 6 - Proceso continuidad de operaciones en crisis

7.1. Prevención

Para asegurar que la respuesta se pueda llevar a cabo de la mejor forma posible, se utilizará una estructura de manejo que atienda de manera oportuna y efectiva los planes administrativos y operativos que se requiere.

Con esta estructura se establecen tres niveles así, Estratégico, Táctico y Tarea, y, estará dada según las necesidades de manejo del incidente y manejo de la crisis. Dentro de cada nivel, los responsables requerirán conocer sus roles específicos a fin de lograr los objetivos del control de la emergencia.

Imagen 7 - Estructura para el control y manejo de emergencia

En los diferentes niveles de la estructura debe haber un líder que entienda sus roles, responsabilidades y funciones. Si los líderes de cada nivel no entienden sus roles y responsabilidades, se presentará confusión que pueden ocasionar una situación que inicialmente estaba catalogada como una emergencia a una crisis.

Estos niveles deben responder y dar apoyo a todos los requerimientos para una respuesta oportuna y efectiva. Deben estar en capacidad de atender la emergencia garantizando los recursos requeridos para su atención, control y continuidad de las operaciones.

7.1.1.Plan preparativo

Para dar atención a las diferentes emergencias que se puedan presentar, se conforman los siguientes niveles de la estructura para el control y manejo:

Nivel de Acción	Equipo	Responsables	Funciones
Estratégico	Equipo de Manejo de Crisis (EMC)	*Gerente de TI - Líder *Coordinador de Infraestructura *Analista de servicios	Coordinar funciones y manejo de la crisis.
Táctico	Equipo de Manejo de Incidentes (EMI)	*Coordinador de Infraestructura - Líder *Analista de servidores y almacenamiento. *Analista de redes y telecomunicaciones	Coordinar procesos y recursos.

		*Auxiliar de redes y telecomunicaciones	
Tarea	Equipo de Apoyo operacional	*Analista de servidores y almacenamiento - Líder *Analista de redes y telecomunicaciones *Auxiliar de redes y telecomunicaciones	Ejecutan las tareas requeridas para llevar a cabo la restauración de la operación.

Tabla 1 - Niveles para control y manejo

7.1.2.Equipo estratégico para el manejo de crisis – EMC

El Equipo Estratégico de Manejo de Crisis proporciona una orientación global de la política para responder al incidente y dar apoyo al Equipo de Manejo de Incidentes. El liderazgo de este grupo estará a cargo del Gerente de TI en Barranquilla o de la persona que éste designe como suplente. Las funciones del Equipo Estratégico de Manejo de Crisis son:

- Dar manejo estratégico y apoyo al Equipo de Manejo del incidente de acuerdo al tipo de escenario presentado.
- Suministrar recursos adicionales de personas, técnicos y especialistas que pudieran necesitar el Equipo de Manejo de Incidentes.
- Proporcionar soporte operativo a la emergencia a nivel local, regional o nacional.
- Permanecer informado, mediante contacto con el Equipo de Manejo de Incidentes, de la evolución de la situación.
- Evaluar y asesorar sobre las necesidades de comunicación a las partes interesadas y la pertinencia de los mismos.
- Servir de exclusivo canal de comunicación con el público en general, previa coordinación con el Equipo de Manejo de Incidentes.

7.1.3.Equipo estratégico manejo de incidente – EMI

El Equipo Estratégico de Manejo de Incidentes EMI, está conformado por el Coordinador de Infraestructura quien es el responsable de la gestión del incidente y todos los colaboradores que lo soportan. El será el único Líder y actuará como tal en la dirección, control y reporte al líder del Equipo de Manejo de Crisis EMC.

El Equipo de Manejo de Incidentes EMI lidera la respuesta estratégica del incidente y está estructurado para cubrir todos los requerimientos; sus roles, responsabilidades y funciones son:

- Identificación y control del incidente.
- Determinación de servicios afectados por el incidente.
- Identificación de cintas para realizar la restauración del servicio afectado.
- Solicitud de cintas de Backup al custodio para restauración de información.
- Activación de centro alterno de trabajo para continuidad de operación.
- Habilitación de canales de contingencia.
- Determinación uso canales de contingencia.
- Restauración de servicios en estado de crisis.

- Rehabilitación de servicios en operación normal.
- Prueba de alternativas a implementar.
- Restauración de operación normal.
- Documentar correctamente el control de una emergencia. Fotos, Actas, Videos, Grabaciones de Voz, etc.
- Contratación de mano de obra personal o solicitud de servicios a empresas contratistas, para el control de la emergencia.
- Gestionar la colaboración de propietarios de predios, donde se requiera adelantar trabajos.
- Divulgar el incidente a la comunidad.
- Implementar medidas tendientes a la conservación del medio ambiente.
- Implementar acciones rápidas y eficaces de limpieza inmediata.
- Atender los medios informativos y recursos para manejar la prensa.
- Establecer y coordinar relación con la prensa
- Emitir comunicaciones formales al interior y exterior del complejo
- Verificar que todas los Plantas estén normalizadas y desarrollen sus actividades adecuadamente, informar dónde se presentan fallas.

Una vez ocurra el incidente que obligue a detener la operación en el complejo Antonio Nariño (Sede Principal en "**la organización**"), es requerido poner en marcha los servicios críticos identificados en el punto **9.1 "*Identificación y valoración de activos*."** siguiendo el orden:

- Identificar las cintas con los Backups realizados más recientes, cerca de la fecha del incidente.
- Determinar viabilidad funcional de las instalaciones principales en el complejo.
- Activar planes alternos de trabajo en momento de crisis.

7.1.4.Equipo de apoyo operacional

Este grupo está formado por las personas de la gerencia y han sido entrenados para atender la respuesta a posibles emergencias. Una de las funciones principales es la de conocer los planes locales de respuesta específicas a emergencias. Igualmente deben conocer perfectamente el sitio, todos los equipos instalados para controlar la emergencia, manejar los equipos y herramientas del sitio conjuntamente con su grupo.

Cada grupo tiene un líder y a su vez este líder deberá estar a cargo del Coordinador de Escena para la coordinación del control de la emergencia.

7.2. Administración de crisis

Durante la etapa de crisis es requerido convocar al equipo de trabajo **EMC, EMI, Equipo de apoyo operacional**, con el fin de dar las pautas e instrucciones a seguir para volver a la operación de la organización.

7.2.1.Detección

Una vez convocado el equipo de trabajo, solamente el Equipo de Manejo de Crisis (**EMC**) estará autorizado para enviar un comunicado a la organización donde se notifica a grosso modo lo sucedido y dando posibles tiempos de respuesta; este comunicado se enviará inicialmente a través de correo electrónico si este servicio se encuentra disponible (ver imagen 8 de ejemplo), en caso contrario se dará la información verbalmente al grupo

directivo de la organización quienes replicarán el mensaje entre sus colaboradores de la misma manera.

CESI

COMUNICADO
31 de marzo de 2017

Inconvenientes técnicos con el acceso al sistema SAP

En estos momentos hay inconvenientes técnicos con el acceso al sistema SAP, por lo cual estamos experimentando dificultades con el acceso al sistema.

Se está trabajando en la solución al incidente. Dejamos a su criterio la puesta en marcha de planes de contingencia operativas, de acuerdo con las condiciones actuales.

Al momento en que se reestablezca el sistema estaremos informando.

Imagen 8 - Ejemplo comunicado a la organización

CESI

MANTENIMIENTO PROGRAMADO DE SERVICIOS INFORMÁTICOS Y DE TELECOMUNICACIONES

INFORMACION SOBRE LA ACTIVIDAD				
FECHA Y HORA INICIAL		FECHA Y HORA FINAL		DURACION
	06:00 P.M.		2:00 A.M.	8 Horas
ACTIVIDADES A REALIZAR		SERVICIOS AFECTADOS		BENEFICIOS ESPERADOS
Migración de la infraestructura tecnológica del servicio de Bases de Datos de las Aplicaciones Corporativas.		Aplicaciones y Portales Web Corporativos: Sharepoints Gerencias, Favim, Logístico, Aviso de Movimientos de Personal, Gestión Estratégica, Evaluación de Desempeño, Emonitor, Viáticos, Sistema Integral de Riesgos.		Mejorar la Disponibilidad, Confiabilidad y Seguridad en el servicio de Base de Datos que soporta las Aplicaciones Corporativas.
NOTAS ADICIONALES				
Agradecemos tomar las medidas de contingencia correspondientes para que durante esta actividad, se puedan llevar a cabo los diferentes procesos del negocio en ausencia de los servicios informáticos afectados.				

Imagen 9 - Notificación mantenimiento de servicio

El **EMI** en compañía del **equipo de apoyo operacional** verificará posibles planes de contingencia para continuar con la operación y se le notificará al **EMC** con el fin de mantener informado en la medida de lo posible a los interesados de la organización para la continuación de las operaciones.

7.2.2. Administración

El **EMI** estará como directo responsable de las acciones a ejecutar para obtener la operación en contingencia de los servicios afectados por la eventualidad, en coordinación

con el **equipo de apoyo operacional** estarán en la labor de habilitar nuevamente los equipos afectados ya sea en el sitio de trabajo normal o en su defecto en el sitio alterno de trabajo que se designe para continuar operaciones bajo emergencia.

El **EMI** se encontrará en la obligación de rendirle reportes o estados de avance de la emergencia detectada e igualmente le solicitará al **EMC** en caso de ser necesario, adquisición de equipos de cómputo para sortear la eventualidad presentada.

7.3. Recuperación

La fase de recuperación será ejecutada por el **equipo de apoyo operacional** el cual será apoyado en sus actividades (adquisición de hardware, software, desplazamiento, alquiler de oficina, etc.) por el **EMI**. El equipo de apoyo operacional deberá levantar un reporte de daños a nivel de hardware y software en caso de ser necesario, esto con el fin de poder dimensionar los esfuerzos para ejecutar la recuperación de la información que se encuentra comprometida al momento del incidente; el único canal de comunicación entre la organización y el custodio de las cintas será el líder del equipo de apoyo operacional quién será el responsable de llevar a cabo dicha actividad e identificar las cintas requeridas para continuar con la operación y la data lo más cercano posible al momento de la eventualidad.

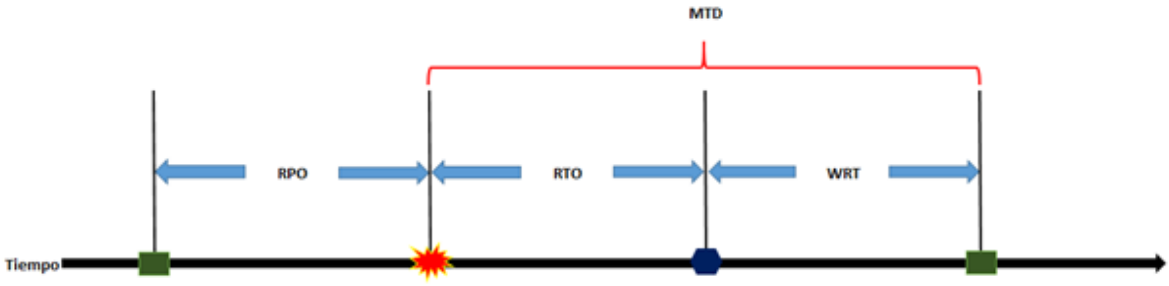

Imagen 10 - Tiempos de recuperación

Una vez identificados los procesos críticos de la organización, es necesario establecer los tiempos de recuperación, los cuales son una serie de componentes correspondientes al tiempo disponible para recuperarse luego de una alteración o falla en el servicio, los tiempos de recuperación de describen a continuación:

Tiempo de recuperación	Descripción
RPO	Magnitud de la pérdida de datos medida en términos de un periodo de tiempo que puede tolerar un proceso de negocio
RTO	Tiempo Disponible para Recuperar Sistemas y/o recursos que han sufrido una alteración.
WRT	Tiempo Disponible para Recuperar Datos Perdidos una vez que los sistemas están reparados. Tiempo de Recuperación de Trabajo.
MTD	Periodo Máximo Tiempo de Inactividad que puede tolerar la Entidad sin entrar en colapso.

Tabla 2 - Definición tiempos de recuperación

Se procede a identificar el MTD, que corresponde al tiempo máximo de inactividad que puede tolerar una organización antes de colapsar y se hace la clasificación a fin de priorizar la recuperación del proceso (servicio). Esto quiere decir que si por ejemplo un proceso tiene

un periodo máximo de tiempo de inactividad (MTD) de un (1) día, este debe tener mayor prioridad para iniciar el evento de recuperación, en razón al poco tiempo de tolerancia de la inactividad, frente a otros que tienen mayor tolerancia.

Prioridad	MTD (Horas)	
	Atención	**Solución**
Alta/Crítica	1.5 horas	Máximo 12 horas
Alta	2 horas	Entre 12 y 16 horas
Media	3 horas	Entre 16 y 20 horas
Baja	4 horas	Máximo 24 horas

Tabla 3 - Tiempos de recuperación

7.3.1. Recuperación del soporte TI

Dentro de los servicios que se deben reestablecer antes de iniciar con las actividades es el de la mesa de servicios CESI "Centro de Servicios Integrales"; estos servicios prestados por el área de TI dentro de sus actividades estarán identificando a través de recepción de llamadas en la línea de atención 611 aquellos servicios que no fueron identificados por el **equipo de apoyo operacional.**

La mesa de servicio CESI tendrá el listado de servicios afectados para contrastar aquellos que no sean identificados por el **equipo de apoyo operacional,** en caso de haber diferencias, notificarán de inmediato al líder del equipo con el fin de incluir dentro de las actividades a desarrollar siempre y cuando se encuentren dentro de los servidores críticos identificados en el **numeral 9.1**.

7.3.2. Recuperación del negocio

Una vez se tienen establecidos los servicios que fueron afectados por el incidente, los equipos de cómputo y recursos de telecomunicación, se procede con Vo.Bo del **EMI** a desplegar las actividades de continuidad de negocio según considere el **equipo de apoyo operacional**, dentro de estas actividades se tiene:

- Desplazamiento a sitio alterno de trabajo.
- Activar canales de comunicación de contingencia.
- Pruebas de disponibilidad y confiabilidad al canal de comunicaciones de contingencia.
- Puesta en marcha de servidores de Backup a la operación.
- Solicitud de cintas magnéticas para restauración de información.
- Configuración de servidores de contingencia para restauración de la información.
- Restauración de información
- Pruebas de integridad a la base de datos restaurada.
- Notificación al personal afectado para reinicio de actividades.
- Supervisión y monitoreo de canales de contingencia.

7.4. Operación en contingencia

Paralelo a las actividades de puesta en marcha o recuperación del negocio, es necesario elevar esfuerzos para realizar la reconstrucción de lo perdido durante el evento de catástrofe; para ello es necesario evaluar la posibilidad de disponer de presupuesto para este tipo de actividades así como de los diferentes recursos /hardware/software/personal, etc. que sean necesarios adquirir/comprar para reanudar actividades normales.

El personal que conforma el equipo de apoyo operacional debe en la medida de lo posible realizar el levantamiento de software/hardware y personal necesario para reanudar las actividades de la organización y notificarle al **EMI** quien a su vez le notificará al **EMC**, previa validación del requerimiento recibido para solicitar adquisición de bienes según el estado y magnitud del evento acontecido.

El proceso de compras debe entonces habilitar su procedimiento para operar durante emergencia, que permita realizar las compras y desembolsos a proveedores para de manera ágil para suplir la necesidad de insumos para la vuelta a la operación normal de la organización.

7.5. Reanudación de operación normal

Una vez adquiridos los diferentes recursos identificados y requeridos por la organización, se debe realizar una ventana de mantenimiento en el cual se hagan por lo menos las siguientes actividades:

- Configuración recursos de hardware adquiridos para operación en productivo.
- Configuración recursos de software adquiridos para operación en productivo.
- Configuración canales de comunicación para operación en productivo.
- Pruebas de integridad a las bases de datos parametrizadas para verificar compatibilidad con las operativas en modo de contingencia.
- Notificación al área usuaria para reanudación de operaciones y disponibilidad de re-trabajo en caso de ser necesario.
- Ventana de mantenimiento para sincronizar servidor de contingencia con servidor productivo.
- Verificación integridad de base de datos con el fin de comprobar la información restaurada y entrada en operación normal.
- Supervisión operación de servidores operativos.
- Suspensión de operaciones en servidor y canales de contingencia.

7.6. Prueba y mantenimiento

Una vez llevado a cabo los puntos anteriores, el **equipo de apoyo operacional, EMI y EMC** retornarán al desarrollo normal de las actividades no sin antes tener en cuenta lo sucedido y documentar en el formato de "**Lecciones aprendidas**", todo lo relacionado con el incidente que sufrió la organización.

Es imperativo realizar un monitoreo constante de las herramientas tecnológicas implementadas para superar el percance presentado durante el incidente, el monitoreo de los componentes debe llevarse a cabo de manera diaria para prevenir a toda costa fallas desde la parte de TI, esta actividad debe ser ejecutada por el personal designado por la organización para tal fin; el personal debe en la medida de lo posible tener una bitácora de sucesos y reuniones periódicas con el fin de tomar acciones correctivas que puedan ayudar a evitar un incidente de igual magnitud o peor.

8. Desarrollo del modelo

Dentro de las actividades a llevar a cabo con ambas metodologías, se tiene entonces el desarrollo del modelo de continuidad operativa de la siguiente manera:

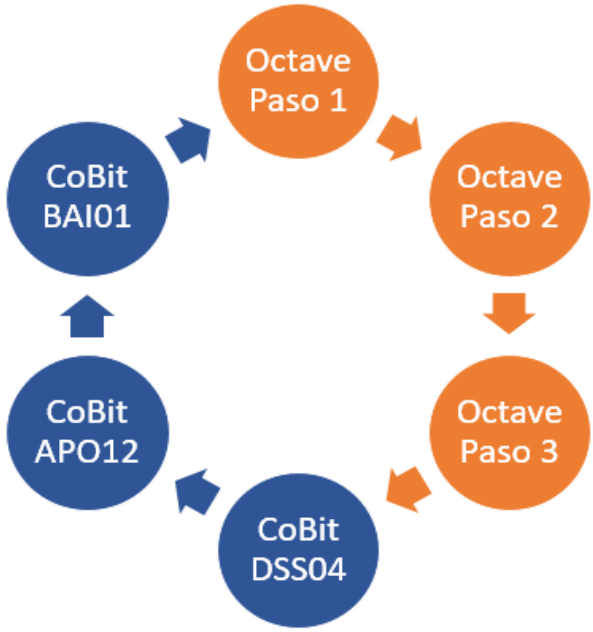

Imagen 11 - Marco metodológico continuidad operativa

Se propone una fusión entre los marcos referenciales de OCTAVE Y CoBit 5, tomando de ambos los puntos que favorecen para cumplir el desarrollo de los objetivos propuestos.

8.1. Paso 1 - Establecer los criterios de la medición del riesgo

El primer paso en el proceso de OCTAVE Allegro establece los criterios organizacionales que se utilizarán para evaluar los efectos de un riesgo para la misión y los objetivos empresariales de una organización.

Estos factores se reflejan en un conjunto de criterios de medición de riesgo que se crea y captura como parte de este paso inicial. Los criterios de medición del riesgo son un conjunto de medidas cualitativas para evaluar los efectos de un riesgo realizado y constituir la base de una evaluación del riesgo de los activos de la información.

El uso de criterios de medición de riesgo consistentes que reflejan con precisión una visión organizacional asegura que las decisiones sobre cómo mitigar el riesgo serán equilibrados entre múltiples activos de información y unidades operativas o departamentales.

Además de evaluar el alcance de un impacto en un área específica, una organización debe reconocer que áreas de impacto son las más significativas para su misión y objetivos de negocio. Por ejemplo, en algunas organizaciones un impacto en la relación con su base de clientes puede ser más significativo que un impacto en su cumplimiento con las regulaciones. Esta priorización de áreas de impacto también se realiza en este paso inicial.

El método OCTAVE Allegro proporciona un conjunto estándar de plantillas de hojas de trabajo para crear estos criterios en varias áreas de impacto, para tal fin se procederá a

trabajar con las plantillas 1 y 7 del apéndice B del documento "*Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*".

Hoja de trabajo 1 **Criterios de medición de riesgos - Reputación y confianza del cliente**

Área de Impacto	Bajo	Moderado	Alto
Reputación (Vendedores)	La reputación del personal es mínimamente afectada. Poco o no esfuerzo o gasto es necesario recuperar.	La reputación del personal de la organización está dañada. No más de usd $ 100K en tiempo y esfuerzo requerido para recuperarse.	La reputación del personal de la organización está severamente dañada. Más de usd $ 100K en tiempo y esfuerzo requerido para recuperarse. La relación con el personal está afectando la reputación con los clientes y la comunidad. Relación deficiente que afecta la eficiencia de la organización y que tiene un efecto notable en la tasa de ventas de la organización.
Reputación (Gerentes)	La reputación del personal es mínimamente afectada. Poco o no esfuerzo o gasto es necesario recuperar.	La reputación entre gerentes se ve afectada, haciendo que los clientes consideren hacer negocio con ellos. La tasa de ventas se ve un poco afectada haciendo que sea necesario más de usd $100K en tiempo y esfuerzo requerido para recuperarse.	La reputación entre gerentes está severamente dañada en la organización y los clientes se rehúsan a tener contacto con ellos para entablar negociaciones. Se estima más de usd $500K en tiempo y esfuerzo para recuperarse pues la tasa de ventas ha sido afectada drásticamente.
Otros: Reputación (Clientes)	La reputación de la organización hacia los clientes es mínimamente afectada. Poco o no esfuerzo o gasto es necesario recuperar.	La reputación entre la comunidad se ve afectada, causando posibles conversaciones en el medio que propician la pérdida de clientes y credibilidad de la organización. Más de usd $100K son requeridos en tiempo y esfuerzo para recuperarse.	La reputación con la comunidad se ve dañada severamente, los clientes rehúsan entablar relación comercial con la organización debido a malas experiencias. Se requieren más de usd $500K en tiempo y esfuerzo para recuperarse pues la tasa de ventas ha sido afectada drásticamente.
Otros: Tasa de ocupación	Una reducción en las ventas mensuales menor al 2%	Una reducción en las ventas mensuales entre el 2% y el 5%	Una reducción en las ventas mensuales mayor al 5%

Tabla 4 - Ejemplo hoja de trabajo 1[14]

[14] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, Mayo 2007, Carnegie Mellon University, página 101.

Hoja de trabajo 7	Hoja de trabajo de priorización del área de impacto
Prioridad	**Área de impacto**
2	Reputación y confianza del cliente
4	Financiero
3	Productividad
5	Seguridad y salud
1	Multas y sanciones legales
n/a	a definir por el usuario

Tabla 5 - Ejemplo Hoja de trabajo 7[15]

8.2. Paso 2 - Desarrollar un perfil para el activo de información.

La metodología de OCTAVE Allegro se centra en los activos de información de la organización y el Paso 2 comienza el proceso de creación de un perfil para esos activos.

Un perfil es una representación de un activo de información que describe sus características únicas, cualidades, características y valor. El proceso de elaboración de perfiles de la metodología asegura que un activo se describe de forma clara y consistente, que existe una definición inequívoca de los límites del activo y que los requisitos de seguridad para el activo están adecuadamente definidos.

El perfil de cada activo se captura en una sola hoja de cálculo que constituye la base para la identificación de amenazas y riesgos en pasos posteriores.

Como objetivo el implementar los workshops propuestos por Octave Allegro con el fin de establecer los criterios de la medición del riesgo, desarrollar un perfil para el activo de información e Identificar los contenedores de los mismos, para estar en la posibilidad de diseñar e implementar el modelo y plan de recuperación para la gerencia de TI.

El método OCTAVE Allegro proporciona un conjunto estándar de plantillas de hojas de trabajo para crear estos criterios en varias áreas de impacto, para tal fin se procederá a trabajar con las plantilla 8 del apéndice B del documento "*Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*".

Hoja de trabajo 8	**Perfil de información crítico**	
Activo Crítico (¿Cuál es el activo de información crítico?)	**Selección de razones** (¿Por qué este activo de información es importante para la organización?)	**Descripción** (¿Cuál es la descripción acordada de este activo de información?)
Información de los clientes de la organización	Mantener la información de los clientes es de vital importancia para la organización y el desarrollo de sus actividades comerciales.	Este activo contiene entre otros; datos de contacto, gerente financiero, gerente de compras, precios manejados con ellos a lo largo de la relación comercial, campañas comerciales realizadas en conjunto, productos adquiridos, precios ofrecidos al cliente.
Dueño(s) (¿Quién es el dueño del activo?)		
El dueño del activo de información es el gerente de ventas de productos industriales (Pedro Pérez)		
Requerimientos de seguridad		

[15] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, Mayo 2007, Carnegie Mellon University, página 113.

(¿Cuáles son los requerimientos de seguridad para este activo de información?)		
Confidencialidad	Sólo personal del área está autorizado a consultar la información de los clientes.	Solamente puede ser consultado por el área de ventas de productos industriales
Integridad	Sólo personal del área de ventas de productos industriales está autorizado a realizar modificaciones al archivo.	Solamente puede ser actualizado por el asesor comercial que atiende al cliente relacionado.
Disponibilidad	El activo debe estar disponible durante el horario laboral.	El activo de información debe estar disponible para gerencia comercial, específicamente para el área de ventas industriales.
	Este activo debe estar disponible durante el horario laboral de 24 horas, 7 días a la semana, 52 semanas al año.	Debido a que algunos clientes se encuentran fuera del país y en otra zona horaria, en algunas ocasiones los vendedores se ven en la necesidad de consultar la información de los mismos en cualquier momento.
Otro	N/A	N/A
Requerimientos de seguridad más importantes (¿Cuál es el requerimiento de seguridad más importante para este activo?)		
☐ **Confidencialidad** ☒ **Integridad** ☐ **Disponibilidad** ☐ **Otro**		

Tabla 6 - Ejemplo Hoja de trabajo 8[16]

8.3. Paso 3 - Identificar los contenedores de los activos de información

Los contenedores describen los lugares donde se almacenan, transportan y procesan los activos de información. Los activos de información residen no sólo en contenedores dentro de los límites de una organización, sino que también residen en contenedores que no están bajo el control directo de la organización. Los riesgos para los contenedores en los que vive el activo de información son heredados por el activo de información.

Por ejemplo, muchas organizaciones externalizan parte, sino toda su infraestructura de TI, a los proveedores de servicios; estos proveedores de servicios gestionan los contenedores que contienen los activos de información de la organización, si un proveedor de servicios no conoce los requisitos de seguridad de un activo de información que se almacena, transporta o procesa en los contenedores que gestiona, los controles necesarios para proteger los activos de información pueden no ser adecuados, exponiendo así los activos a riesgo.

Este problema puede llegar a ser aún más pronunciado si el proveedor de servicios a su vez contrata otros servicios (como el almacenamiento de datos) con proveedores de servicios adicionales que pueden ser desconocidos para el propietario del recurso de información. Por lo tanto, para obtener un perfil de riesgo adecuado de un activo de información, una organización debe identificar todos los lugares donde sus activos de información son almacenados, transportados o procesados, estén o no dentro del control directo de la organización.

En el Paso 3 del método OCTAVE Allegro se identifican todos los contenedores en los que se almacena, transporta y procesa un activo, sea interno o externo, en este paso, el equipo de análisis asigna un activo de información a todos los contenedores en los que vive,

[16] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, Mayo 2007, Carnegie Mellon University, página 115, 116.

definiendo así los límites y circunstancias únicas que deben examinarse para determinar el riesgo.

El método OCTAVE Allegro proporciona un conjunto estándar de plantillas de hojas de trabajo para crear estos criterios en varias áreas de impacto, para tal fin se procederá a trabajar con la plantilla 8 del apéndice B del documento "*Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*".

Hoja De Trabajo 9a	**Mapa De Riesgos Activo De Información (Técnico)**
Interno	
Descripción Del Contendor	**Propietario**
El archivo de contacto de clientes reside en el clúster del área comercial (gerencia de productos industriales), se encuentra en el servido WS2008(1) y su réplica en el WS2008(2), es un archivo que puede ser accedido solamente por el área comercial y por el personal de la misma gerencia; el servidor actualmente cuenta con S.O Windows Server 2012	Departamento de TI
Todas las actualizaciones son llevadas a cabo en las tablas de retención documental de la organización, las cuales se encuentra en el servidor WS2008 (3) y su réplica en el WS2008 (4).	Departamento de TI
Externo	
Descripción Del Contendor	**Propietario**
Los datos corporativos de los clientes almacenados en cámara de comercio para ejecución de negocios relevantes, así como consulta de los mismos para apertura de crédito.	Cámara de comercio

Tabla 7 - Ejemplo Hoja de trabajo 9a[17]

Hoja De Trabajo 9b	**Mapa De Riesgos Activo De Información (Físico)**
Interno	
Descripción del contenedor	**Propietario**
Copias del maestro de clientes impreso, con la información base para contacto de los mismos.	Área comercial
Información financiera del cliente, relacionada con estados financieros y embargos	Área de tesorería
Externo	
Descripción del contenedor	**Propietario**
Impresión de información enviada al cliente a través de correo electrónico	Área de tesorería

Tabla 8 - Ejemplo Hoja de trabajo 9b[18]

[17] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, Mayo 2007, Carnegie Mellon University, página 117.
[18] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, Mayo 2007, Carnegie Mellon University, página 119.

Hoja De Trabajo 9c	Mapa De Riesgos Activo De Información (Personas)
Personal Interno	
Nombre o rol/responsabilidad	**Departamento o unidad**
Gerente	Gerencia de productos industriales
Especialista de ventas	Gerencia de productos industriales
Analista de tesorería	Gerencia de tesorería
Analista de cuentas por pagar	Gerencia de contabilidad
Personal Externo	
Contratista, vendedor, especialista, etc.	**Organización**
Personal contratado para el transporte de las cintas de back up de la organización	MTI

Tabla 9 - Ejemplo Hoja de trabajo 9c[19]

Esta labor dará como resultado las entradas para iniciar el análisis que se desea realizar en los dominios de CoBit 5; de esta manera se podrá entonces culminar con el ciclo de revisión y acciones a tomar referente a los activos de información, una vez se identifique la información obtenida en cada uno de los pasos seleccionados de la metodología de Octave y el framework CoBit 5.

Para seguir con el análisis de los activos de información, sus componentes, repositorios y demás, los siguientes dominios fueron seleccionados para alcanzar el objetivo propuesto en el presente trabajo de grado:

8.4. DSS04 "Gestionar la Continuidad"

El dominio **DSS04** consiste en "*establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.*

Se busca continuar las operaciones críticas para el negocio y mantener la disponibilidad de la información a un nivel aceptable para la empresa ante el evento de una interrupción significativa."[20]

Este dominio tomará como entrada el **paso 1, 2 y 3** de **Octave**, donde se procederá a gestionar la continuidad de la organización.

Se busca con este proceso tener la información crítica para el negocio y que esta esté disponible en línea con los niveles de servicio mínimos requeridos, para el ejercicio a realizar, se llevarán a cabo las siguientes actividades enunciadas por el dominio DSS04.02[21]

Prácticas de Gestión	Entrada		Salida	
DSS04.02 Mantener una estrategia de continuidad. Evaluar las opciones de gestión de la continuidad de negocio y escoger una estrategia de continuidad viable y efectiva en coste, que pueda asegurar la continuidad y recuperación de la	**De**	**Descripción**	**Descripción**	**A**
	Paso 1, 2 y 3 de Octave	Causas raíz relacionadas con riesgos Impacto de los riesgos	Análisis de impacto en el negocio	APO12.02

[19] Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, Mayo 2007, Carnegie Mellon University, página 119.
[20] ISACA, COBIT® 5: Procesos Catalizadores, 2012, página 185
[21] ISACA, COBIT® 5: Procesos Catalizadores, 2012, página 187

empresa frente a un desastre u otro incidente mayor o disrupción.				
Actividades				
Identificar escenarios potenciales probables que puedan dar pie a eventos que puedan causar incidentes disruptivos importantes.				
Realizar un análisis de impacto en el negocio para evaluar el tiempo de una disrupción en funciones críticas del negocio y el efecto que tendría en ellas				
Establecer el tiempo mínimo necesario para recuperar un proceso de negocio y su soporte de TI, basándose en una duración aceptable de interrupción del negocio y la interrupción máxima tolerable				
Analizar la probabilidad de amenazas que puedan causar pérdidas de continuidad de negocio e identificar medidas que puedan reducir la probabilidad y el impacto, mejorando la prevención e incrementando la resiliencia.				
Analizar los requerimientos de continuidad para identificar las posibles estrategias de negocio y opciones técnicas				
Determinar las condiciones y los responsables de decisiones clave que puedan causar la invocación de los planes de continuidad				

Tabla 10 - Actividades a desarrollar dominio DSS04

8.5. APO12 "Gestionar el Riesgo"

El dominio **APO12** consiste en "*identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.*

El propósito de éste proceso es integrar la gestión de riesgos empresariales relacionados con TI con la gestión de riesgos empresarial general (ERM) y equilibrar los costes y beneficios de gestionar riesgos empresariales relacionados con TI."[22]

Este dominio tomará como entrada lo obtenido al momento de ejecutar el **DSS04** y obtener el análisis de impacto en el negocio.

Se busca con este proceso tener el riesgo relacionado con el proceso de TI identificado, analizado y gestionado, así como un perfil de riesgo actual y completo, para el ejercicio a realizar, se llevarán a cabo las siguientes actividades enunciadas por el dominio APO12.02[23]

Prácticas de Gestión	Entrada		Salida	
APO12.02 Analizar el riesgo.	**De**	**Descripción**	**Descripción**	**A**
Desarrollar información útil para soportar las decisiones relacionadas con el riesgo que tomen en cuenta la relevancia para el negocio de los factores de riesgo	DSS04.02	Análisis de Impacto en el negocio	Resultados de análisis de riesgos	BAI01.10
Actividades				
Definir la amplitud y profundidad apropiada para los esfuerzos en análisis de riesgos, considerando todos los factores de riesgo y la criticidad en el negocio de los activos. Establecer el alcance del análisis de riesgos después de llevar a cabo un análisis coste-beneficio.				
Construir y actualizar regularmente escenarios de riesgo de TI, que incluyan escenarios compuestos en cascada y/o tipos de amenaza coincidentes y desarrollar expectativas para actividades de control específicas, capacidades para detectar y otras medidas de respuesta				

[22] ISACA, COBIT® 5: Procesos Catalizadores, 2012, página 107
[23] ISACA, COBIT® 5: Procesos Catalizadores, 2012, página 109

Estimar la frecuencia y magnitud de pérdida o ganancia asociada con escenarios de riesgo de TI. Tener en cuenta todos los factores de riesgo que apliquen, evaluar controles operacionales conocidos y estimar niveles de riesgo residual.
Comparar el riesgo residual con la tolerancia al riesgo e identificar exposiciones que puedan requerir una respuesta al riesgo
Analizar el coste-beneficio de las opciones de respuesta al riesgo potencial, tales como evitar, reducir/mitigar, transferir/compartir y aceptar y explotar/capturar. Proponer la respuesta al riesgo óptima.

Tabla 11 - Actividades a desarrollar dominio APO12

8.6. BAI01 "Gestión de programas de proyectos"

El dominio **BAI01** consiste en gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia corporativa. Iniciar, planificar, controlar y ejecutar programas y proyectos y cerrarlos con una revisión post-implementación.

El propósito de este proceso es alcanzar los beneficios de negocio y reducir el riesgo de retrasos y costes inesperados y el deterioro del valor, mediante la mejora de las comunicaciones y la involucración de usuarios finales y de negocio, asegurando el valor y la calidad de los entregables del proyecto y maximizando su contribución al portafolio de servicios e inversiones.[24]

Este dominio tomará como entrada lo obtenido al momento de ejecutar el **APO12** y obtener la información requerida para la gestión del riesgo.

Se busca con este proceso tener un plan acción donde se aprecie el cumplimiento de requerimientos de capacidad, rendimiento y disponibilidad así como número y porcentaje de cuestiones de disponibilidad, rendimiento y capacidad no resueltos durante un tiempo determinado; se propondrá inicialmente una medición mensual.

Llevando a cabo estas actividades se podrá tener entonces un ciclo continuo de revisión de los activos de información, donde se puede entonces tener al finalizar el ciclo, un proyecto o plan de trabajo que permita realizar controles y mejoras en los activos identificados, así como en sus contenedores; para el ejercicio a realizar, se llevarán a cabo las siguientes actividades enunciadas por el dominio BAI01.10[25]

Prácticas de Gestión	Entrada		Salida	
BAI01.10 Gestionar el riesgo de los programas y proyectos. Eliminar o minimizar los riesgos específicos asociados con los programas y proyectos mediante un proceso sistemático de planificación, identificación, análisis, respuesta, supervisión y control de las áreas o eventos que tienen el potencial de causar cambios no deseados. Los riesgos enfrentados por la administración del programa y los proyectos deberían ser	**De**	**Descripción**	**Descripción**	**A**
	APO12.02	Resultado del análisis de riesgos	Plan de gestión de riesgos del proyecto	Interno
			Resultado de la evaluación de riesgos del proyecto	Interno

[24] ISACA, COBIT® 5: Procesos Catalizadores, 2012, página 119
[25] ISACA, COBIT® 5: Procesos Catalizadores, 2012, página 125

establecidos y registrados en un único punto.				
Actividades				
Establecer un enfoque de gestión de riesgo de proyectos alineado con el marco de referencia de ERM. Asegurar que este enfoque incluya la identificación, análisis, respuesta, mitigación, supervisión y control del riesgo.				
Asignar la responsabilidad para ejecutar el proceso de gestión del riesgo de los proyectos de la entidad al personal con las capacidades adecuadas y asegurar que está incorporado en las prácticas de desarrollo de la solución. Considerar asignar este perfil a un equipo independiente, especialmente si es necesario un punto de vista objetivo o el proyecto se considera crítico.				
Realizar un análisis de riesgo del proyecto para identificar y cuantificar el riesgo de manera continua durante el proyecto. Gestionar y comunicar el riesgo adecuadamente dentro de la estructura de gobierno del proyecto.				
Reevaluar el riesgo del proyecto periódicamente, incluyendo al inicio de cada fase de un proyecto importante y como parte de las evaluaciones de solicitudes de cambios importantes.				
Identificar los propietarios de las acciones para evitar, aceptar o mitigar el riesgo.				

Tabla 12 - Actividades a desarrollar dominio BAI01

9. Implementación del modelo

El cronograma que se propone a continuación presenta como finalidad obtener los siguientes entregables con el fin de saber el estado actual de la organización y aquello a lo que se le debe prestar atención:

- Identificación de Activos
- Identificación de Amenazas
- Identificación de Prácticas Actuales

Dichos entregables son obtenidos con los primeros pasos del modelo propuesto y se encuentra basado en la metodología Octave.

Nombre	Duracion
Continuidad de operaciones	180 days
Analisis	11 days
Cronograma	11 days
Elaboracion del cronograma	1 day
Diseño de la Solucion	10 days
Definición situación actual	5 days
Elaboracion del diseño de la solucion	5 days
Desarrollo	165 days
Levantamiento de información organizacional	70 days
Reunión con lideres de proceso	10 days
Reunión con lideres de TI	10 days
Identificación de activos	5 days
Identificación de amenazas	5 days
Identificación de prácticas actuales	10 days
Análisis de vulnerabilidades	30 days
Levantamiento de información tecnológica	80 days
Reunión con lideres de proceso	10 days
Reunión con lideres de TI	10 days
Identificación de activos	10 days
Identificación de amenazas	10 days
Identificación de prácticas actuales	10 days
Análisis de vulnerabilidades	30 days
Estrategia plan y desarrollo	15 days
Identificación de riesgos	5 days
Estrategias de protección	5 days
Planes de mitigación	5 days
Implementación	2 days
Verificacion del Cumplimiento de Objetivos	1 day
Puesta en Marcha	1 day
Cierre	2 days
Verificación de documentación generada	2 days

Tabla 13 - Cronograma de actividades

Teniendo en cuenta el cronograma de actividades, se desea identificar los activos de información que hacen parte en el proceso de respaldo de información en empresas del

sector químico, de igual manera conocer los contenedores de dichos activos, conocer los diferentes riesgos a los que están expuestos, los controles que se tienen para la disminución de éstos y posibles mejoras que se puedan implementar a futuro para una mejor gestión de los activos de información del proceso antes mencionado.

9.1. Identificación y valoración de activos.

A través de reuniones realizadas e implementando la metodología OCTAVE, se efectúa la identificación Top-Down de los activos de información a través de workshops con la línea gerencia de primer nivel.

En las reuniones a celebrar en esta primera instancia se tiene como finalidad el obtener un listado de los activos de información que considera la alta dirección, mandos medios y nivel operacional de la organización como críticos e importantes para la continuidad de negocio, se espera tener reuniones no mayores a 1 hora pues se tiene como establecido este tiempo como óptimo para esta fase del proyecto.

Una vez se identifican los activos de información importantes y dándoles una valoración a los mismos con el personal de alta dirección (primer nivel), se procede a realizar la misma actividad con los mandos medios (segundo nivel) así como con la(s) persona(s) que consideren los participantes de primer nivel como relevantes; culminada esta actividad, se realiza entonces el mismo proceso con el personal de tercer nivel (nivel operativo) quienes ayudarán a confirmar los activos identificados en los niveles anteriores y posiblemente a identificar activos desconocidos por personal de primer y segundo nivel; este tercer nivel estará integrado también por personal de TI, que si bien no son propietarios de la información, si son custodios de la misma y pueden aportar una identificación de activos de una forma más granular y conveniente para el desarrollo de esta actividad.

Una vez realizado el ejercicio de identificación de activos de información, validación de los activos encontrados y consolidación de los mismos, se procede presentar el listado a la alta dirección para su conocimiento, pues es posible que no se haya tenido en cuenta durante el ejercicio algún activo de información durante los workshops.

Una vez realizada la actividad anterior, se logra identificar los activos de información críticos para la organización y se determina con ayuda del DBA la ubicación de los mismos para crear planes de acción que ayuden a continuar con la operación en caso de un incidente de fuerza mayor que obligue a detener las operaciones en el complejo principal; se obtiene como resultado el siguiente listado:

9.1.1. Relación de archivos y carpetas a respaldar

Servicio	Servidor
BASE DE DATOS HP DATA PROTECTOR	2UX73606GM-24
CORREO CORPORATIVO	BL-MAIL0150
BASES DE DATOS SQLSERVER 2005	BL-SQLSERVER83, BL-SQLSERVER0258
SISTEMA DE CONTROL DE ACCESO LEGACY	BL-SCA74

Tabla 14 - Relación de archivos y carpetas a respaldar

9.1.2.Relación de servidores virtuales a respaldar

Servicio	Servidor
SHAREPOINT CORPORATIVO	BL-SHAREPOINT0127
SERVIDOR DE LICENCIAS Y APPS	MCVAPPSRV0180
BASES DE DATOS PORTALES PHP	MCVLNXDB0168
APLICACIONES LOTUS DOMINO	MCVAPPDOMINO68
CONTROLADOR DE DOMINIO PRIMARIO	MCVBAQDC0189
CONTROLADOR DE DOMINIO SECUNDARIO	MCVBAQDC0288
BASES DE DATOS SQLSERVER 2012	MCVSQLSRV0120
SISTEMA DE CONTROL DE ACCESO	MCVSCA61
GESTION DOCUMENTAL	MCVSGDFS0138
SERVIDOR DE ARCHIVOS	MCVFS0177
SERVIDOR WEB PORTALES PHP	MCVLNXWEB0145
MONITOREO DE INFRAESTRUCTURA TI	LNXPORTAL83
MONITOREO DE INFRAESTRUCTURA TI	MCVLNXMON0124
WEB INTERNO	BL-INTRANET32
WEB EXTERNO	BL-WEB90
TERMINAL SERVICES	MCVTS0152
ADMINISTRACIÓN PLANTA TELEFONICA	MCVOMNIOXE0199
SERVICIO DE IMPRESIÓN	MCVPRINTER84
ANTIVIRUS	MCVSEC0145
BLACKBERRY ENTERPRISE	MCVBES10257
LOTUS TRAVELER	MCVTRAVELER41
GESTION DE ACTIVOS INFORMATICOS	MCVDISCOVERY20
CORREO CORPORATIVO SEGUNDO NODO	BL-MAIL0228
LOTUS SAMETIME	MCVST38
SERVICIO EASY SALES COMERCIAL	MCVESS0182
SERVICIO DE ACTUALIZACIÓN DE WINDOWS	MCVRDPSUS0167
ANTIVIRUS	MCVSEC0250
GESTION DOCUMENTAL WEB	MCVSGDW0184
WEB INTERNO	MCVWEB0180
VMWARE VCENTER	MCVCENTER0168
ACRONIS BACKUPS	MCVBKP0247

Tabla 15 - Relación de servidores virtuales a respaldar

9.1.3. Relación de servidores virtuales a respaldar (Calidad y Desarrollo)

Servicio	Servidor
IBM CONTENT	CONTENT82
GESTION DOCUMENTAL	DOCMGR51
SERVIDOR DE APLICACIONES	ERP_APP35
SOFTWARE RH LEGADO	OLIVIA58
SERVIDOR DE APLICACIONES	BL-APPSERVER90
HP SERVICE MANAGER	BL-HPSM0180
BASE DE DATOS ERP LEGADO	DBCLUS0190
BASE DE DATOS ERP LEGADO	DBSERVER0161
DESARROLLO ERP LEGADO	ERP_DESA40
DESARROLLO APLICACIONES LOTUS	MCVLOTUSDESA0151
DESARROLLO SIST. GESTION DOCUMENTAL	MCVSGDESA0172
DESARROLLO SISTEMA SWIFT	MCVSWIFTDESA0125

DESARROLLO SERVICIO WEB	MCVWEBDESA0139
DESARROLLO INTRANET	BL-INTRANET32
DESARROLLO SQLSERVER 2005	MCVSQLDESA0178
DESARROLLO SQLSERVER 2012	MCVSQL12DESA0189
CALIDAD WEB EXTERNO	MCVLNXCAL0183
DESARROLLO WEB EXTERNO	MCVLNXSAND0183
DESARROLLO ERP LEGADO	HOBBES70
DESARROLLO PRUEBAS WIN XP	MPC-DAIT0161

Tabla 16 - Relación de servidores virtuales a respaldar (Calidad y Desarrollo)

Luego de realizar el levantamiento de la información referente a los servidores críticos en la organización, se identifican los siguientes como objeto de atención pues son aquellos que contienen los servicios más importantes para el negocio:

- CONTENT82
- DOCMGR51
- MCVFS0177
- BL-MAIL0150
- BL-MAIL0228

9.2. Identificación de amenazas.

Luego de haber llevado a cabo las reuniones con el DBA de la organización, se identifican las siguientes amenazas para con los servidores señalados como críticos:

- Versión de sistemas operativos obsoletos en servidores que se encuentran en operación.
- Cercanía del datacenter principal de **la organización** a áreas de riesgo en la empresa.
- Falta de conocimiento para procesos de restauración a personal Backup del área encargada.
- Manuales de proceso de respaldo de información desactualizados.
- Falta de adiestramiento del personal para actuar en momento de crisis, no se hacen simulacros.
- No se cuenta con un sitio alterno de trabajo para restaurar la información en caso de una eventualidad.
- Posible saturación del canal de contingencia al momento de ser utilizado como principal en caso de una eventualidad.
- Posible falla en canal de comunicación principal y secundario al estar ubicados en la misma zona geográfica.
- Desconocimiento de configuración en canal de contingencia para entrar en operación debido a eventualidad.
- Presupuesto poco o nulo para atención de desastres TI.
- Procesos lentos para la compra de equipos en caso de sortear una eventualidad.
- Altos tiempos de respuesta del custodio de las cintas en sitios alternos de trabajo.

9.3. Identificación de prácticas actuales.

A través de reuniones celebradas con el DBA de la empresa, se identifica que **la organización** tiene instaladas las siguientes herramientas para realizar los respaldos de los servidores listados en los puntos **9.1.1**, **9.1.2** y **9.1.3**:

- **HP DATA PROTECTOR:** Esta herramienta respalda los pocos servidores físicos que están pronto a ser virtualizados o migrados por su obsolescencia, estos son BL-SQLSERVER83, BL-SQLSERVER0258 y BL-SCA74.

- **VEEAM BACKUP AND REPLICATION**: Esta herramienta respalda mediante imágenes los servidores que son máquinas virtuales en la infraestructura VMWARE, pero solo para el Clúster Productivo.

- **ACRONIS BACKUP & RECOVERY**: Con esta herramienta se respalda a través de imágenes, los servidores que son máquinas virtuales en la infraestructura VMWARE, pero solo para los Clusters de Desarrollo y Legado. De igual manera se le efectúa el respaldo a los servidores Físicos MCVBKP0247, MCVSWIFTDESA0125, MCVASTBAR857 y MAVASTBAR029863.

Teniendo en cuenta lo anterior, es posible entonces mencionar los siguientes aspectos de las herramientas de respaldo:

- La herramienta *HP Data Protector* se encuentra integrado con las librerías de cintas HP **MSL6000 LTO3** y **HP AUTOLOADER LTO6,** esto con el fin de almacenar todos los respaldos programados en esta herramienta.

- *VEEAM BACKUP AND REPLICATION* está integrado con la librería de cintas **HP AUTOLOADER LTO6** para almacenar todos respaldos programados en esta herramienta.

Por otra parte, la estrategia de rotación de cintas que está implementada es "**Abuelo, Padre e Hijo**", dicha rotación se detalla de la siguiente manera:

- Se realizan respaldos diarios de lunes a viernes, donde cada respaldo tiene retención de Seis (6) días. Es decir, cada respaldo diario tiene vigencia de una semana aproximadamente en las cintas donde se almacena.

- Se realizan respaldos semanales los sábados y domingos, donde cada respaldo tiene retención de veintisiete (27) días. Es decir, cada respaldo semanal tiene vigencia de un mes aproximadamente en las cintas donde se almacena.

- El último domingo de cada mes, se toma también como respaldo mensual de ese mes, el cual pasa a tener una retención de Un (1) año. Es decir, dicho respaldo es semanal y el mensual.

- El respaldo del último domingo de diciembre, se toma como el respaldo anual, teniendo una retención de cinco (5) años. Es decir, este respaldo sería un respaldo Semanal, Mensual y Anual.

El control de los horarios se encuentra detallado en el documento "*BACKUPS*

MANAGER.xlsx"[26].

Dentro de las actividades realizadas por el DBA referente a lo que tiene que ver con respaldo de información, se establece que diariamente se debe revisar en las herramientas de respaldo si los Backups configurados se han ejecutado sin inconvenientes, en caso contrario, se deben tomar acciones según sea el caso.[27]

9.4. Vulnerabilidades de la organización.

Luego de realizar la identificación de amenazas se procede a verificar las posibles vulnerabilidades que puede tener nuestro proceso objeto de estudio, encontrando las siguientes:

- **Vulnerabilidades Físicas**
  - Servidores antiguos.
  - Ubicación de Datacenter en zona de riesgo químico.

- **Vulnerabilidades Naturales**
  - Ubicación del data center cerca de fuentes fluviales susceptibles a desbordamiento.
  - Ubicación del data center en planta química con altos índices contaminantes.

- **Vulnerabilidades de Hardware**
  - Centro de datos centralizado, no se cuenta con puntos alternos de trabajo que puedan entrar en operación en caso de desastres.
  - Procesos lentos para sustituir equipos de cómputo deteriorados ante una eventualidad

- **Vulnerabilidades de Software**
  - Sistemas operativos obsoletos instalados y operativos en servidores productivos.
  - Pocas pruebas de intrusión para software operativo.
  - Caída del servicio.

- **Vulnerabilidades Humanas**
  - Falta de capacitación a personal Backup en el proceso de respaldo que puedan brindar apoyo al momento de ejecutar el proceso.
  - Documentación desactualizada de procesos.
  - Claves compartidas de 1 mismo usuario en 3 funcionarios diferentes.

9.5. Identificación de componentes clave.

Luego de llevar a cabo el ejercicio de identificación de activos de información, y validar el estado de los repositorios de los mismos, se identifica que es necesario realizar un análisis de amenazas y vulnerabilidades a los activos de información importantes para el proceso de

[26] El documento de referencia no será detallado debido a confidencialidad del mismo y al no ser objeto de estudio del presente documento.
[27] Para más información se puede consultar el documento "Plan inicial de recuperación infraestructura IT"

respaldo de Backups que se desea establecer en la organización.

9.6. Identificación de vulnerabilidades de la organización.

Podemos entender las vulnerabilidades como las debilidades asociadas a los activos de información que se hacen efectivas cuando una amenaza la materializa; éstas no son causa necesariamente de daño, sino que son condiciones que pueden hacer que una amenaza afecte a un activo de información en particular.

Para cada amenaza identificada se debe realizar un análisis de riesgo para identificar las vulnerabilidades, como resultado de esta actividad se obtiene el primer componente para la estimación del nivel de **impacto** de cada uno de los activos de información, y para calcularlo se utilizará una valoración cualitativa cuyos rangos se definen de la siguiente manera:

Valor	Descripción
5	Perjuicios que ponen en riesgo la continuidad del negocio y representan sanciones y/o pérdidas significativas para la organización
4	Perjuicios extensivos que generan pérdida en la capacidad de producción, y, que generan riesgos asociados importantes
3	Perjuicios que se controlan localmente y con asistencia externa, y, que pueden generar riesgos asociados
2	Pocos perjuicios que se controlan local e inmediatamente
1	No generan perjuicios

Tabla 17 - Nivel de Impacto

De igual manera, se debe realizar una definición de escala cualitativa para los valores relacionados a la **probabilidad**, los cuales se definen de la siguiente manera:

Valor	Descripción
0.0 - 0.3	Ocurre cada 5 años
0.4 - 0.5	Ocurre 1 vez al año
0.6 - 0.7	Ocurre semestralmente
0.8-1	Ocurre mensualmente

Tabla 18 - Nivel de probabilidad

Teniendo en cuenta las tablas anteriores, procedemos a definir la valoración del riesgo, el cual se calculará de la siguiente manera:

Riesgo= Impacto* Probabilidad

Teniendo en cuenta el producto de esa operación, se definen los valores cualitativos con la siguiente tabla:

Valor	Descripción
4.1-5	Riesgo Alto
2.5-4	Riesgo Medio
1-2.4	Riesgo Bajo

Tabla 19 - Valores del riesgo

Lo que permite entonces definir nuestra matriz de calor de la siguiente manera:

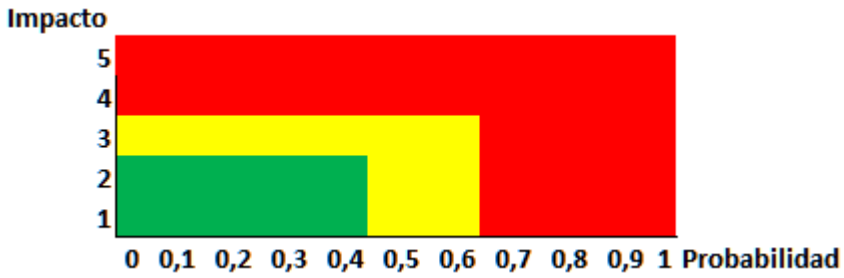

Imagen 12 - Semáforo Impacto vs Probabilidad

La ejecución del levantamiento de información e identificación de amenazas para el proceso de respaldo de información en la gerencia AIT, arrojó resultado interesantes que eran desconocidos por la alta dirección; dentro de ellos, se pudo detectar altos niveles del impacto que se puede tener al materializarse un riesgo, así como altas probabilidades.

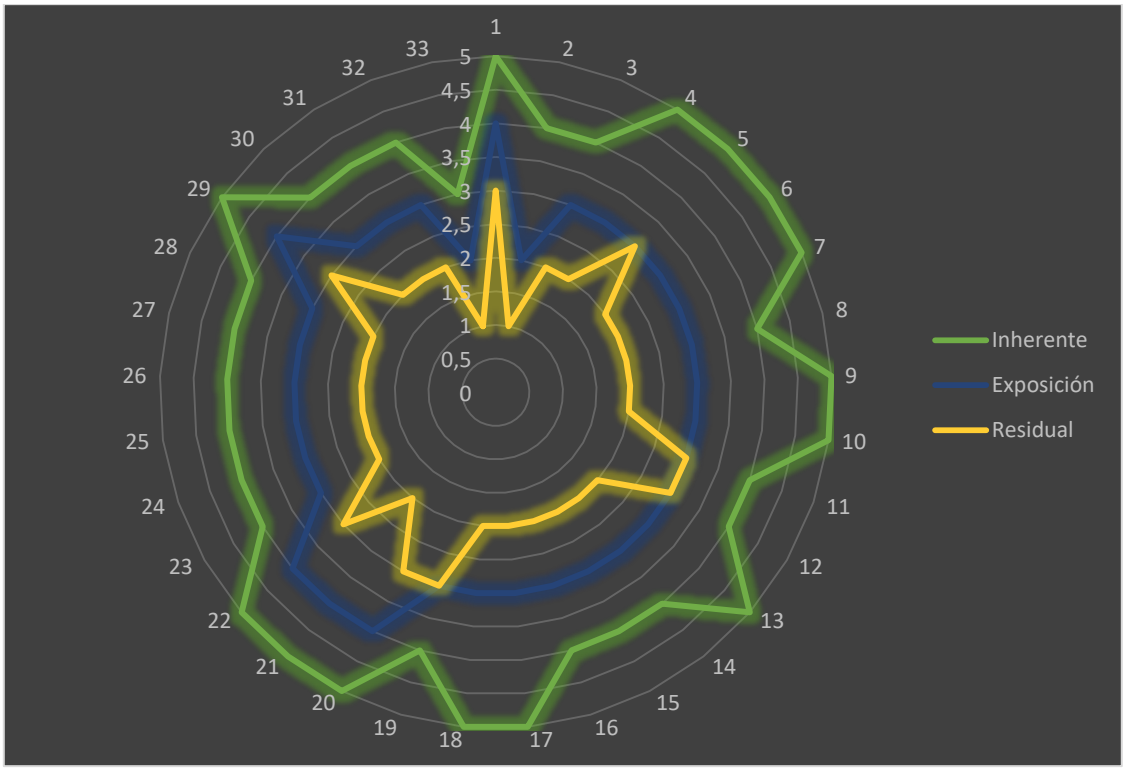

Gráfico 1 - Impacto del riesgo en la organización

Se puede apreciar en el **gráfico 1**, que el nivel de riesgo de exposición es moderado, y los controles que se tienen implementados actualmente pueden y deben ser mejorados, en la medida de lo posible llevándolos a cero.

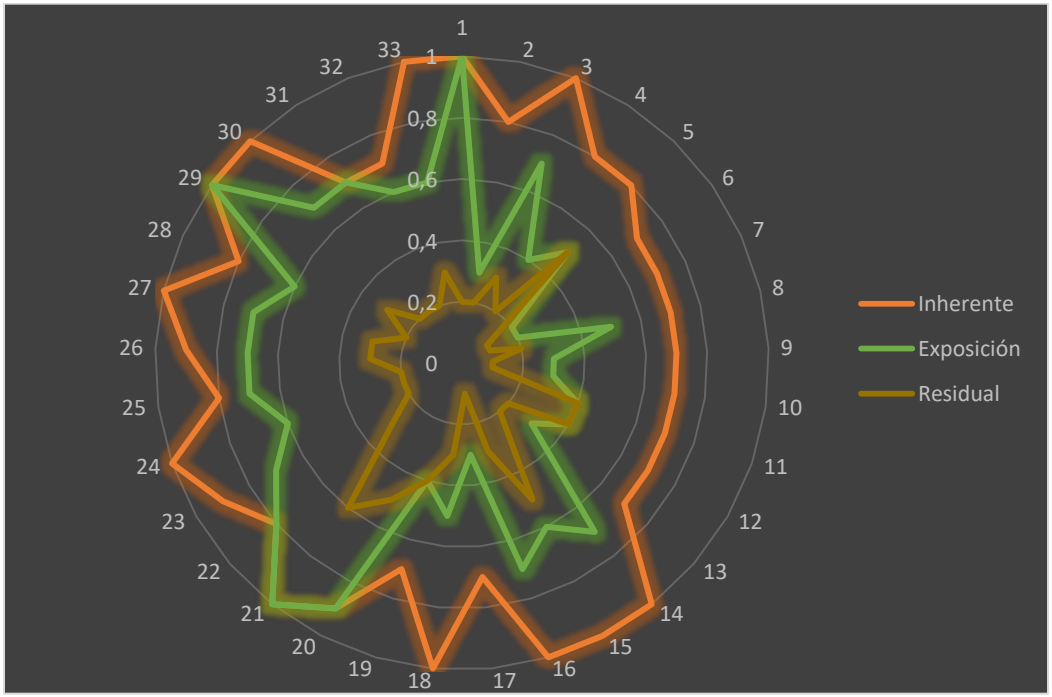

Gráfico 2 - Probabilidad materialización del riesgo

En el tema de probabilidad, evidenciado en el **gráfico 2**, igualmente se aprecia un nivel medio-alto, nos indica que es inminente la materialización del riesgo que se ha detectado en el ejercicio de identificación de activos de información, amenazas y vulnerabilidades.

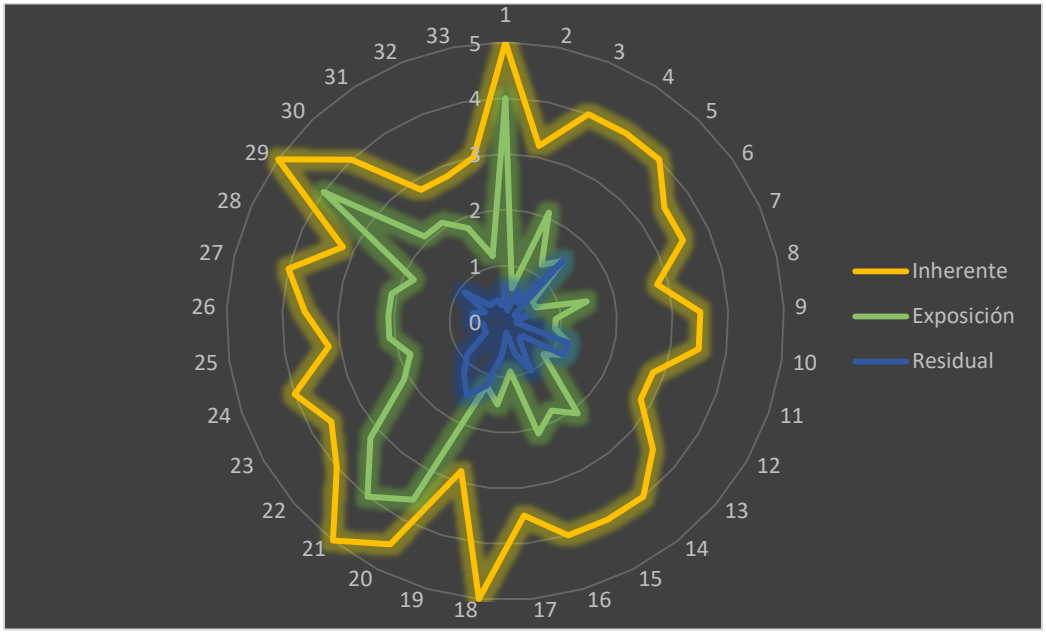

Gráfico 3 - Valoración del riesgo en la organización

Teniendo en cuenta las imágenes anteriores, el **gráfico 3** confirma la información encontrada, es imperativo realizar acciones correctivas y preventivas para la mitigación de las amenazas y reducción de la probabilidad con el fin de obtener un impacto menor.

Para más detalle puede consultarse la información consignada en el **Anexo 1** y el **Anexo 2** del presente documento.

10. Conclusiones

A través de la actividad ejecutada se pudo evidenciar la necesidad por parte de la organización de establecer y diseñar un procedimiento para la continuidad de negocio desde el punto de vista de TI; si bien se tienen establecidos mecanismos que garanticen la continuidad del negocio desde la parte operativa y producción, se tenía una falencia para garantizar las operaciones a nivel nacional pues la disponibilidad de la información no había sido considerada como necesaria para seguir en la operación.

El resultado del trabajo ejecutado brindó alternativas de solución para la problemática que se tenía al momento de realizar esfuerzos para garantizar la continuidad operativa de los sistemas de información; el levantamiento de información ayudó a determinar aquellos recursos indispensables para la organización que permiten seguir con sus actividades cotidianas aún en momentos de crisis.

El apoyo ofrecido inicialmente por la alta dirección fue un poco escéptico, no obstante, al ir obteniendo los resultados del trabajo realizado, se pudo determinar la necesidad que presentaba la organización para realizar inversiones en equipos informáticos; esto, ofreció a la alta dirección un panorama más certero para ejecución de inversiones y culminó con el apoyo total para la ejecución del proyecto y dio pie para implementación de planes operativos para ejecutar la misma actividad año tras año.

Fue posible luego de la ejecución del proyecto tener un inventario actualizado de los activos de información críticos para la organización, esto brindó la posibilidad para la gerencia de TI de mejorar y optimizar sus procesos de ejecución de respaldo, así como inclusión de servidores que se tenían fuera del alcance pues se consideraban contenedores de información no relevante que podía ser reestablecida en cualquier momento y no era clave para la continuidad operativa.

Bibliografía

[1] ISACA, CoBit 5: Procesos Catalizadores, 2012.

[2] ISACA, CoBit 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa, Rolling Meadows, 2012.

[3] R. A. S. J. F. Y. L. R. &. W. W. R. Caralli, Introducing octave allegro: Improving the information security risk assessment process, PITTSBURGH: CARNEGIE-MELLON UNIV SOFTWARE ENGINEERING INST, 2007.

11. Anexos

11.1. Anexo 1 Valoración de Riesgos

Servidor	Amenaza	Vulnerabilidad Físicas	Impacto	Probabilidad	Riesgo
CONTENT82 DOCMGR51 MCVFS0177 BL-MAIL0150 BL-MAIL0228	1. Versión de sistemas operativos obsoletos en servidores que se encuentran en operación.	Servidores antiguos	5	1	5
	2. Cercanía del datacenter principal de la organización a áreas de riesgo en la empresa.	Ubicación de Datacenter en zona de riesgo químico	4	0,8	3,2
	5. Falta de adiestramiento del personal para actuar en momento de crisis, no se hacen simulacros.	Servidores antiguos	4	1	4
	6. No se cuenta con un sitio alterno de trabajo para restaurar la información en caso de una eventualidad.	Ubicación de Datacenter en zona de riesgo químico	5	0,8	4
	8. Posible falla en canal de comunicación principal y secundario al estar ubicados en la misma zona geográfica.	Ubicación de Datacenter en zona de riesgo químico	5	0,8	4

Tabla 20 - Valoración vulnerabilidades físicas.

Servidor	Amenaza	Vulnerabilidad Naturales	Impacto	Probabilidad	Riesgo
CONTENT82 DOCMGR51 MCVFS0177 BL-MAIL0150 BL-MAIL0228	2. Cercanía del datacenter principal de la organización a áreas de riesgo en la empresa.	Ubicación del datacenter cerca de fuentes fluviales susceptibles a desbordamiento	5	0,7	3,5
	2. Cercanía del datacenter principal de la organización a áreas de riesgo en la empresa.	Ubicación del datacenter en planta química con altos índices contaminantes	5	0,7	3,5
	5. Falta de adiestramiento del personal para actuar en momento de crisis, no se hacen simulacros.	Ubicación del datacenter cerca de fuentes fluviales susceptibles a desbordamiento	4	0,7	2,8
	6. No se cuenta con un sitio alterno de trabajo para restaurar la información en caso de una eventualidad.	Ubicación del datacenter cerca de fuentes fluviales susceptibles a desbordamiento	5	0,7	3,5
	6. No se cuenta con un sitio alterno de trabajo para restaurar la información en caso de una eventualidad.	Ubicación del datacenter en planta química con altos índices contaminantes	5	0,7	3,5
	8. Posible falla en canal de comunicación principal y secundario al estar ubicados en la misma zona geográfica.	Ubicación del datacenter cerca de fuentes fluviales susceptibles a desbordamiento	4	0,7	2,8
	8. Posible falla en canal de comunicación principal y secundario al estar ubicados en la misma zona geográfica.	Ubicación del datacenter en planta química con altos índices contaminantes	4	0,7	2,8

Tabla 21 - Valoración vulnerabilidades naturales

Servidor	Amenaza	Vulnerabilidad Hardware	Impacto	Probabilidad	Riesgo
CONTENT82 DOCMGR51 MCVFS0177 BL-MAIL0150 BL-MAIL0228	2. Cercanía del datacenter principal de la organización a áreas de riesgo en la empresa.	Centro de datos centralizado, no se cuenta con puntos alternos de trabajo que puedan entrar en operación en caso de desastres.	5	0,7	3,5
	3. Falta de conocimiento para procesos de restauración a personal Backup del área encargada.	Procesos lentos para sustituir equipos de cómputo deteriorados ante una eventualidad	4	1	4
	4. Manuales de proceso de respaldo de información desactualizados.	Procesos lentos para sustituir equipos de cómputo deteriorados ante una eventualidad	4	1	4
	5. Falta de adiestramiento del personal para actuar en momento de crisis, no se hacen simulacros.	Procesos lentos para sustituir equipos de cómputo deteriorados ante una eventualidad	4	1	4
	6. No se cuenta con un sitio alterno de trabajo para restaurar la información en caso de una eventualidad.	Centro de datos centralizado, no se cuenta con puntos alternos de trabajo que puedan entrar en operación en caso de desastres.	5	0,7	3,5
	6. No se cuenta con un sitio alterno de trabajo para restaurar la información en caso de una eventualidad.	Procesos lentos para sustituir equipos de cómputo deteriorados ante una eventualidad	5	1	5
	8. Posible falla en canal de comunicación principal y secundario al estar ubicados en la misma zona geográfica.	Centro de datos centralizado, no se cuenta con puntos alternos de trabajo que puedan entrar en operación en caso de desastres.	4	0,7	2,8

Tabla 22 - Valoración vulnerabilidades hardware

Servidor	Amenaza	Vulnerabilidad Software	Impacto	Probabilidad	Riesgo
CONTENT82 DOCMGR51 MCVFS0177 BL-MAIL0150 BL-MAIL0228	1. Versión de sistemas operativos obsoletos en servidores que se encuentran en operación.	Sistemas operativos obsoletos instalados y operativos en servidores productivos	5	0,9	4,5
	1. Versión de sistemas operativos obsoletos en servidores que se encuentran en operación.	Pocas pruebas de intrusión para software operativo.	5	1	5
	1. Versión de sistemas operativos obsoletos en servidores que se encuentran en operación.	Caída del servicio	5	0,8	4
	3. Falta de conocimiento para procesos de restauración a personal Backup del área encargada.	Sistemas operativos obsoletos instalados y operativos en servidores productivos	4	0,9	3,6
	3. Falta de conocimiento para procesos de restauración a personal Backup del área encargada.	Pocas pruebas de intrusión para software operativo.	4	1	4
	3. Falta de conocimiento para procesos de restauración a personal Backup del área encargada.	Caída del servicio	4	0,8	3,2
	5. Falta de adiestramiento del personal para actuar en momento de crisis, no se hacen simulacros.	Sistemas operativos obsoletos instalados y operativos en servidores productivos	4	0,9	3,6
	5. Falta de adiestramiento del personal para actuar en momento de crisis, no se hacen simulacros.	Pocas pruebas de intrusión para software operativo.	4	1	4
	5. Falta de adiestramiento del personal para actuar en momento de crisis, no se hacen simulacros.	Caída del servicio	4	0,8	3,2

Tabla 23 - Valoración vulnerabilidades software

Servidor	Amenaza	Vulnerabilidad Humanas	Impacto	Probabilidad	Riesgo
CONTENT82 DOCMGR51 MCVFS0177 BL-MAIL0150 BL-MAIL0228	1. Versión de sistemas operativos obsoletos en servidores que se encuentran en operación.	Falta de capacitación a personal Backup en el proceso de respaldo que puedan brindar apoyo al momento de ejecutar el proceso	5	1	5
	3. Falta de conocimiento para procesos de restauración a personal Backup del área encargada.	Falta de capacitación a personal Backup en el proceso de respaldo que puedan brindar apoyo al momento de ejecutar el proceso	4	1	4
	3. Falta de conocimiento para procesos de restauración a personal Backup del área encargada.	Documentación desactualizada de procesos.	4	0,7	2,8
	5. Falta de adiestramiento del personal para actuar en momento de crisis, no se hacen simulacros.	Documentación desactualizada de procesos.	4	0,7	2,8
	9. Altos tiempos de respuesta del custodio de las cintas en sitios alternos de trabajo.	Falta de capacitación a personal Backup en el proceso de respaldo que puedan brindar apoyo al momento de ejecutar el proceso	3	1	3

Tabla 24 - Valoración vulnerabilidades humanas

11.2. Anexo 2 Tratamiento de Riesgo

Amenaza	Clase de Vulnerabilidad	Vulnerabilidad	Efectos Posibles	Controles Existentes	Impacto	Probabilidad	Riesgo de Exposición
1. Versión de sistemas operativos obsoletos en servidores que se encuentran en operación.	Física	Servidores antiguos	Falla en los equipos que se encuentran dado servicio a la operación en la organización.	*Se tiene diseñado un plan de migración con fecha límite 2018 con el fin de adquirir nuevas licencias que permitan migrar portales y herramientas operativas a ambientes con S.O más recientes.	4	1	4
2. Cercanía del datacenter principal de la organización a áreas de riesgo en la empresa.	Física	Ubicación de Datacenter en zona de riesgo químico	Pérdida de la información en los servidores debido a deterioro acelerado.	*El datacenter está implementado con puertas de seguridad y sistemas de emergencia que permiten la operación en momento de presentar amenaza física, no obstante no se tiene implementado aún el sitio alterno de trabajo.	2	0,3	0,6
5. Falta de adiestramiento del personal para actuar en momento de crisis, no se hacen simulacros.	Física	Servidores antiguos	Desconocimiento en implementación de actualizaciones a equipos obsoletos, así como falta de parches (actualizaciones) disponibles pues han salido de soporte.	*Se tiene diseñado un plan de capacitación para el equipo de infraestructura que da soporte a los servicios en la organización, así como simulacros de emergencia para verificar tiempos de respuesta del personal y capacidad de reacción del mismo.	3	0,7	2,1
6. No se cuenta con un sitio alterno de trabajo para restaurar la información en caso de una eventualidad.	Física	Ubicación de Datacenter en zona de riesgo químico	Pérdida de la información en los servidores debido a catástrofe en sitio de trabajo.	*Se tiene diseñado un plan de implementación del sitio alterno de trabajo en Bogotá, con el fin de respaldar el datacenter principal de la organización.	3	0,4	1,2

8. Posible falla en canal de comunicación principal y secundario al estar ubicados en la misma zona geográfica.	Física	Ubicación de Datacenter en zona de riesgo químico	Deterioro en las fibras de comunicación en los canales principal y secundario debido a exposición a material corrosivo en la ubicación del data center principal.	*Se tiene contratado un proveedor con alta disponibilidad, el servicio de internet está con la opción de canal principal y canal de contingencia con el mismo proveedor.	3	0,5	1,5
2. Cercanía del datacenter principal de la organización a áreas de riesgo en la empresa.	Naturales	Ubicación del datacenter cerca de fuentes fluviales susceptibles a desbordamiento	Inundación de instalaciones donde se encuentran los servidores.	*El datacenter está implementado con puertas de seguridad y sistemas de emergencia que permiten la operación en momento de presentar amenaza física, no obstante, no se tiene implementado aún el sitio alterno de trabajo.	3	0,2	0,6
2. Cercanía del datacenter principal de la organización a áreas de riesgo en la empresa.	Naturales	Ubicación del datacenter en planta química con altos índices contaminantes	Pérdida de la información en los servidores debido a deterioro acelerado.	*El datacenter está implementado con puertas de seguridad y sistemas de emergencia que permiten la operación en momento de presentar amenaza física, no obstante no se tiene implementado aún el sitio alterno de trabajo.	3	0,2	0,6
5. Falta de adiestramiento del personal para actuar en momento de crisis, no se hacen simulacros.	Naturales	Ubicación del datacenter cerca de fuentes fluviales susceptibles a desbordamiento	Falla de los empleados para aplicar contingencias o métodos para continuar con la operación luego de un incidente de magnitud alta.	*Se tiene diseñado un plan de capacitación para el equipo de infraestructura que da soporte a los servicios en la organización, así como simulacros de emergencia para verificar tiempos de respuesta del personal y capacidad de reacción del mismo.	3	0,5	1,5

6. No se cuenta con un sitio alterno de trabajo para restaurar la información en caso de una eventualidad.	Naturales	Ubicación del datacenter cerca de fuentes fluviales susceptibles a desbordamiento	Pérdida de la información en los servidores debido a catástrofe en sitio de trabajo.	*Se tiene diseñado un plan de implementación del sitio alterno de trabajo en Bogotá, con el fin de respaldar el datacenter principal de la organización.	3	0,3	0,9
6. No se cuenta con un sitio alterno de trabajo para restaurar la información en caso de una eventualidad.	Naturales	Ubicación del datacenter en planta química con altos índices contaminantes	Pérdida de la información en los servidores debido a catástrofe en sitio de trabajo.	*Se tiene diseñado un plan de implementación del sitio alterno de trabajo en Bogotá, con el fin de respaldar el datacenter principal de la organización.	3	0,3	0,9
8. Posible falla en canal de comunicación principal y secundario al estar ubicados en la misma zona geográfica.	Naturales	Ubicación del datacenter cerca de fuentes fluviales susceptibles a desbordamiento	Deterioro en las fibras de comunicación en los canales principal y secundario debido a filtraciones de agua por inundaciones en el sitio de trabajo principal.	*Se tiene contratado un proveedor con alta disponibilidad, el servicio de internet está con la opción de canal principal y canal de contingencia con el mismo proveedor.	3	0,4	1,2
8. Posible falla en canal de comunicación principal y secundario al estar ubicados en la misma zona geográfica.	Naturales	Ubicación del datacenter en planta química con altos índices contaminantes	Deterioro en las fibras de comunicación en los canales principal y secundario debido a exposición a material corrosivo en la ubicación del data center principal.	*Se tiene contratado un proveedor con alta disponibilidad, el servicio de internet está con la opción de canal principal y canal de contingencia con el mismo proveedor.	3	0,4	1,2
2. Cercanía del datacenter principal de la organización a áreas de riesgo en la empresa.	Hardware	Centro de datos centralizado, no se cuenta con puntos alternos de trabajo que puedan entrar en operación en caso de desastres.	Pérdida de la información en los servidores debido a deterioro acelerado.	*El datacenter está implementado con puertas de seguridad y sistemas de emergencia que permiten la operación en momento de presentar amenaza física, no obstante no se tiene implementado aún el sitio alterno de trabajo.	3	0,3	0,9

3. Falta de conocimiento para procesos de restauración a personal Backup del área encargada.	Hardware	Procesos lentos para sustituir equipos de cómputo deteriorados ante una eventualidad	Errores al momento de restaurar información necesaria para las operaciones del negocio.	*Se tiene documentado el procedimiento para restauración de Backups en los equipos actuales, no obstante, solo 1 empleado sabe hacer el proceso o ha practicado hacerlo.	3	0,7	2,1
4. Manuales de proceso de respaldo de información desactualizados.	Hardware	Procesos lentos para sustituir equipos de cómputo deteriorados ante una eventualidad	Pérdida de la información debido a procesos ineficientes de respaldo de información con equipos no compatibles.	*Se tiene la documentación de los procesos, sin embargo no se ha actualizado en más de 5 años por lo que posiblemente la información consignada es obsoleta.	3	0,6	1,8
5. Falta de adiestramiento del personal para actuar en momento de crisis, no se hacen simulacros.	Hardware	Procesos lentos para sustituir equipos de cómputo deteriorados ante una eventualidad	Pérdida de la información debido a procesos ineficientes de respaldo de información con equipos no compatibles.	*Se tiene diseñado un plan de capacitación para el equipo de infraestructura que da soporte a los servicios en la organización, así como simulacros de emergencia para verificar tiempos de respuesta del personal y capacidad de reacción del mismo.	3	0,7	2,1
6. No se cuenta con un sitio alterno de trabajo para restaurar la información en caso de una eventualidad.	Hardware	Centro de datos centralizado, no se cuenta con puntos alternos de trabajo que puedan entrar en operación en caso de desastres.	Inoperatividad del servicio, inutilizando la disponibilidad de la información.	*Se tiene diseñado un plan de implementación del sitio alterno de trabajo en Bogotá, con el fin de respaldar el datacenter principal de la organización.	3	0,3	0,9
6. No se cuenta con un sitio alterno de trabajo para restaurar la información en caso de una eventualidad.	Hardware	Procesos lentos para sustituir equipos de cómputo deteriorados ante una eventualidad	Inoperatividad del servicio, inutilizando la disponibilidad de la información.	*Se tiene diseñado un plan de implementación del sitio alterno de trabajo en Bogotá, con el fin de respaldar el datacenter principal de la organización.	3	0,5	1,5
8. Posible falla en canal de comunicación principal y secundario al estar ubicados en la misma zona geográfica.	Hardware	Centro de datos centralizado, no se cuenta con puntos alternos de trabajo que puedan entrar en operación en	Pérdida de la comunicación entre sedes que ayudan a la incomunicación y deterioro en la integridad de los	*Se tiene contratado un proveedor con alta disponibilidad, el servicio de internet está con la opción de canal principal y canal de	3	0,4	1,2

		caso de desastres.	datos.	contingencia con el mismo proveedor.			
1. Versión de sistemas operativos obsoletos en servidores que se encuentran en operación.	Software	Sistemas operativos obsoletos instalados y operativos en servidores productivos	Software desactualizado que conlleva a lentitud en las operaciones y posibles reprocesos al tener programas sin soporte que pueden fallar en cualquier momento.	*Se tiene diseñado un plan de migración con fecha límite 2018 con el fin de adquirir nuevas licencias que permitan migrar portales y herramientas operativas a ambientes con S.O más recientes.	4	0,9	3,6
1. Versión de sistemas operativos obsoletos en servidores que se encuentran en operación.	Software	Pocas pruebas de intrusión para software operativo.	Software con falencias de seguridad que puede ser foco para ataques informáticos.	*Se tiene diseñado un plan de migración con fecha límite 2018 con el fin de adquirir nuevas licencias que permitan migrar portales y herramientas operativas a ambientes con S.O más recientes.	4	1	4
1. Versión de sistemas operativos obsoletos en servidores que se encuentran en operación.	Software	Caída del servicio	Inoperatividad del servicio, inutilizando la disponibilidad de la información.	*Se tiene diseñado un plan de migración con fecha límite 2018 con el fin de adquirir nuevas licencias que permitan migrar portales y herramientas operativas a ambientes con S.O más recientes.	4	0,8	3,2
3. Falta de conocimiento para procesos de restauración a personal Backup del área encargada.	Software	Sistemas operativos obsoletos instalados y operativos en servidores productivos	Errores en la restauración del servicio y poca confiabilidad en la información almacenada.	*Se tiene documentado el procedimiento para restauración de Backups en los equipos actuales, no obstante, solo 1 empleado sabe hacer el proceso o ha practicado hacerlo.	3	0,7	2,1
3. Falta de conocimiento para procesos de restauración a personal Backup del área encargada.	Software	Pocas pruebas de intrusión para software operativo.	Software vulnerable a ataques informáticos que pueden poner en riesgo las operaciones de la organización.	*Se tiene documentado el procedimiento para restauración de Backups en los equipos actuales, no obstante, solo 1 empleado sabe hacer el proceso o ha practicado hacerlo.	3	0,6	1,8

3. Falta de conocimiento para procesos de restauración a personal Backup del área encargada.	Software	Caída del servicio	Errores al momento de restaurar información necesaria para las operaciones del negocio.	*Se tiene documentado el procedimiento para restauración de Backups en los equipos actuales, no obstante, solo 1 empleado sabe hacer el proceso o ha practicado hacerlo.	3	0,7	2,1
5. Falta de adiestramiento del personal para actuar en momento de crisis, no se hacen simulacros.	Software	Sistemas operativos obsoletos instalados y operativos en servidores productivos	Software desactualizado que conlleva a lentitud en las operaciones y posibles reprocesos al tener programas sin soporte que pueden fallar en cualquier momento.	*Se tiene diseñado un plan de capacitación para el equipo de infraestructura que da soporte a los servicios en la organización, así como simulacros de emergencia para verificar tiempos de respuesta del personal y capacidad de reacción del mismo.	3	0,7	2,1
5. Falta de adiestramiento del personal para actuar en momento de crisis, no se hacen simulacros.	Software	Pocas pruebas de intrusión para software operativo.	Software con falencias de seguridad que puede ser foco para ataques informáticos.	*Se tiene diseñado un plan de capacitación para el equipo de infraestructura que da soporte a los servicios en la organización, así como simulacros de emergencia para verificar tiempos de respuesta del personal y capacidad de reacción del mismo.	3	0,7	2,1
5. Falta de adiestramiento del personal para actuar en momento de crisis, no se hacen simulacros.	Software	Caída del servicio	Inoperatividad del servicio, inutilizando la disponibilidad de la información.	*Se tiene diseñado un plan de capacitación para el equipo de infraestructura que da soporte a los servicios en la organización, así como simulacros de emergencia para verificar tiempos de respuesta del personal y capacidad de reacción del mismo.	3	0,6	1,8

1. Versión de sistemas operativos obsoletos en servidores que se encuentran en operación.	Humanas	Falta de capacitación a personal Backup en el proceso de respaldo que puedan brindar apoyo al momento de ejecutar el proceso	Errores al momento de dar soporte/mantenimiento a los servicios cuando se requiera interactuar con servidores obsoletos.	*Se tiene diseñado un plan de migración con fecha límite 2018 con el fin de adquirir nuevas licencias que permitan migrar portales y herramientas operativas a ambientes con S.O más recientes.	4	1	4
3. Falta de conocimiento para procesos de restauración a personal Backup del área encargada.	Humanas	Falta de capacitación a personal Backup en el proceso de respaldo que puedan brindar apoyo al momento de ejecutar el proceso	Errores en el proceso de restauración de información.	*Se tiene documentado el procedimiento para restauración de Backups en los equipos actuales, no obstante, solo 1 empleado sabe hacer el proceso o ha practicado hacerlo.	3	0,7	2,1
3. Falta de conocimiento para procesos de restauración a personal Backup del área encargada.	Humanas	Documentación desactualizada de procesos.	Errores en el proceso de restauración de información.	*Se tiene documentado el procedimiento para restauración de Backups en los equipos actuales, no obstante, solo 1 empleado sabe hacer el proceso o ha practicado hacerlo.	3	0,7	2,1
5. Falta de adiestramiento del personal para actuar en momento de crisis, no se hacen simulacros.	Humanas	Documentación desactualizada de procesos.	Errores en el proceso de restauración de información.	*Se tiene diseñado un plan de capacitación para el equipo de infraestructura que da soporte a los servicios en la organización, así como simulacros de emergencia para verificar tiempos de respuesta del personal y capacidad de reacción del mismo.	3	0,6	1,8
9. Altos tiempos de respuesta del custodio de las cintas en sitios alternos de trabajo.	Humanas	Falta de capacitación a personal Backup en el proceso de respaldo que puedan brindar apoyo al momento de ejecutar el proceso	Confusión al momento de hacer restauración de la información debido a desconocimiento en el proceso de manejo de cintas.	*Se tiene implementado un SLA con el proveedor custodio de las cintas para traer lo que se le requiera en menos de 3 horas.	2	0,6	1,2

Tabla 25 - Riesgo de exposición

Amenaza	Clase de Vulnerabilidad	Vulnerabilidad	Efectos Posibles	Valoración Residual			
				Control Propuesto	Impacto	Probabilidad	Riesgo Residual
1. Versión de sistemas operativos obsoletos en servidores que se encuentran en operación.	Física	Servidores antiguos	Falla en los equipos que se encuentran dado servicio a la operación en la organización.	*Migrar software crítico a servidores nuevos, que tengan garantía del fabricante.	3	0,2	0,6
2. Cercanía del datacenter principal de la organización a áreas de riesgo en la empresa.	Física	Ubicación de Datacenter en zona de riesgo químico	Pérdida de la información en los servidores debido a deterioro acelerado.	*Habilitar un sitio alterno de trabajo, geográficamente lejos del sitio actual con el fin de ser activado en caso de sufrir una eventualidad en el datacenter principal de la organización	1	0,2	0,2
5. Falta de adiestramiento del personal para actuar en momento de crisis, no se hacen simulacros.	Física	Servidores antiguos	Desconocimiento en implementación de actualizaciones a equipos obsoletos, así como falta de parches (actualizaciones) disponibles pues han salido de soporte.	*Verificar los simulacros y tiempos de respuesta en los ejercicios de simulación ejecutados, con el fin de mejorar en la medida de lo posible la reacción del personal involucrado.	2	0,3	0,6
6. No se cuenta con un sitio alterno de trabajo para restaurar la información en caso de una eventualidad.	Física	Ubicación de Datacenter en zona de riesgo químico	Pérdida de la información en los servidores debido a catástrofe en sitio de trabajo.	*Verificar que el sitio alterno de trabajo cumpla con la demanda que se tendrá al momento de entrar en operación en caso de tener una situación de emergencia, esto con el fin de afinar aquellos detalles que sean vitales para su óptimo funcionamiento.	2	0,2	0,4
8. Posible falla en canal de comunicación principal y secundario al estar ubicados en la misma zona geográfica.	Física	Ubicación de Datacenter en zona de riesgo químico	Deterioro en las fibras de comunicación en los canales principal y secundario debido a exposición a material corrosivo en la ubicación del data center principal.	*No aplica	3	0,5	1,5
2. Cercanía del datacenter principal de la organización a áreas de riesgo en la empresa.	Naturales	Ubicación del datacenter cerca de fuentes fluviales susceptibles a desbordamiento	Inundación de instalaciones donde se encuentran los servidores.	*Habilitar un sitio alterno de trabajo, geográficamente lejos del sitio actual con el fin de ser activado en caso de sufrir una eventualidad en el datacenter principal de la organización	2	0,1	0,2

2. Cercanía del datacenter principal de la organización a áreas de riesgo en la empresa.	Naturales	Ubicación del datacenter en planta química con altos índices contaminantes	Pérdida de la información en los servidores debido a deterioro acelerado.	*Habilitar un sitio alterno de trabajo, geográficamente lejos del sitio actual con el fin de ser activado en caso de sufrir una eventualidad en el datacenter principal de la organización	2	0,1	0,2
5. Falta de adiestramiento del personal para actuar en momento de crisis, no se hacen simulacros.	Naturales	Ubicación del datacenter cerca de fuentes fluviales susceptibles a desbordamiento	Falla de los empleados para aplicar contingencias o métodos para continuar con la operación luego de un incidente de magnitud alta.	*Verificar los simulacros y tiempos de respuesta en los ejercicios de simulación ejecutados, con el fin de mejorar en la medida de lo posible la reacción del personal involucrado.	2	0,2	0,4
6. No se cuenta con un sitio alterno de trabajo para restaurar la información en caso de una eventualidad.	Naturales	Ubicación del datacenter cerca de fuentes fluviales susceptibles a desbordamiento	Pérdida de la información en los servidores debido a catástrofe en sitio de trabajo.	*Verificar que el sitio alterno de trabajo cumpla con la demanda que se tendrá al momento de entrar en operación en caso de tener una situación de emergencia, esto con el fin de afinar aquellos detalles que sean vitales para su óptimo funcionamiento.	2	0,1	0,2
6. No se cuenta con un sitio alterno de trabajo para restaurar la información en caso de una eventualidad.	Naturales	Ubicación del datacenter en planta química con altos índices contaminantes	Pérdida de la información en los servidores debido a catástrofe en sitio de trabajo.	*Verificar que el sitio alterno de trabajo cumpla con la demanda que se tendrá al momento de entrar en operación en caso de tener una situación de emergencia, esto con el fin de afinar aquellos detalles que sean vitales para su óptimo funcionamiento.	2	0,1	0,2
8. Posible falla en canal de comunicación principal y secundario al estar ubicados en la misma zona geográfica.	Naturales	Ubicación del datacenter cerca de fuentes fluviales susceptibles a desbordamiento	Deterioro en las fibras de comunicación en los canales principal y secundario debido a filtraciones de agua por inundaciones en el sitio de trabajo principal.	*No aplica	3	0,4	1,2
8. Posible falla en canal de comunicación principal y secundario al estar ubicados en la misma zona geográfica.	Naturales	Ubicación del datacenter en planta química con altos índices contaminantes	Deterioro en las fibras de comunicación en los canales principal y secundario debido a exposición a material corrosivo en la	*No aplica	3	0,4	1,2

			ubicación del data center principal.				
2. Cercanía del datacenter principal de la organización a áreas de riesgo en la empresa.	Hardware	Centro de datos centralizado, no se cuenta con puntos alternos de trabajo que puedan entrar en operación en caso de desastres.	Pérdida de la información en los servidores debido a deterioro acelerado.	*Habilitar un sitio alterno de trabajo, geográficamente lejos del sitio actual con el fin de ser activado en caso de sufrir una eventualidad en el datacenter principal de la organización	2	0,2	0,4
3. Falta de conocimiento para procesos de restauración a personal Backup del área encargada.	Hardware	Procesos lentos para sustituir equipos de cómputo deteriorados ante una eventualidad	Errores al momento de restaurar información necesaria para las operaciones del negocio.	*Capacitar a mínimo 2 empleados adicionales en la ejecución del proceso de restauración de Backups en la herramienta, con el fin de eliminar la dependencia de 1 solo empleado en momentos álgidos para la ejecución de dicho proceso.	2	0,2	0,4
4. Manuales de proceso de respaldo de información desactualizados.	Hardware	Procesos lentos para sustituir equipos de cómputo deteriorados ante una eventualidad	Pérdida de la información debido a procesos ineficientes de respaldo de información con equipos no compatibles.	*Llevar a cabo la actualización del documento desactualizado, de igual manera, levantar aquellos procesos que se estén ejecutando sin documentación para formalizarlos y socializarlos con el equipo de trabajo.	2	0,5	1
5. Falta de adiestramiento del personal para actuar en momento de crisis, no se hacen simulacros.	Hardware	Procesos lentos para sustituir equipos de cómputo deteriorados ante una eventualidad	Pérdida de la información debido a procesos ineficientes de respaldo de información con equipos no compatibles.	*Verificar los simulacros y tiempos de respuesta en los ejercicios de simulación ejecutados, con el fin de mejorar en la medida de lo posible la reacción del personal involucrado.	2	0,3	0,6
6. No se cuenta con un sitio alterno de trabajo para restaurar la información en caso de una eventualidad.	Hardware	Centro de datos centralizado, no se cuenta con puntos alternos de trabajo que puedan entrar en operación en caso de desastres.	Inoperatividad del servicio, inutilizando la disponibilidad de la información.	*Verificar que el sitio alterno de trabajo cumpla con la demanda que se tendrá al momento de entrar en operación en caso de tener una situación de emergencia, esto con el fin de afinar aquellos detalles que sean vitales para su óptimo funcionamiento.	2	0,1	0,2

6. No se cuenta con un sitio alterno de trabajo para restaurar la información en caso de una eventualidad.	Hardware	Procesos lentos para sustituir equipos de cómputo deteriorados ante una eventualidad	Inoperatividad del servicio, inutilizando la disponibilidad de la información.	*Verificar que el sitio alterno de trabajo cumpla con la demanda que se tendrá al momento de entrar en operación en caso de tener una situación de emergencia, esto con el fin de afinar aquellos detalles que sean vitales para su óptimo funcionamiento.	2	0,3	0,6
8. Posible falla en canal de comunicación principal y secundario al estar ubicados en la misma zona geográfica.	Hardware	Centro de datos centralizado, no se cuenta con puntos alternos de trabajo que puedan entrar en operación en caso de desastres.	Pérdida de la comunicación entre sedes que ayudan a la incomunicación y deterioro en la integridad de los datos.	*No aplica	3	0,4	1,2
1. Versión de sistemas operativos obsoletos en servidores que se encuentran en operación.	Software	Sistemas operativos obsoletos instalados y operativos en servidores productivos	Software desactualizado que conlleva a lentitud en las operaciones y posibles reprocesos al tener programas sin soporte que pueden fallar en cualquier momento.	*Migrar software crítico a servidores con sistema operativo recientes, que cuenten con parches de seguridad actualizados y garantía por parte del fabricante.	3	0,5	1,5
1. Versión de sistemas operativos obsoletos en servidores que se encuentran en operación.	Software	Pocas pruebas de intrusión para software operativo.	Software con falencias de seguridad que puede ser foco para ataques informáticos.	*Crear un plan de acción para el año 2018, con el fin de llevar a cabo esta actividad e informar sus resultados para creación de controles y/o diseño de soluciones	2	0,6	1,2
1. Versión de sistemas operativos obsoletos en servidores que se encuentran en operación.	Software	Caída del servicio	Inoperatividad del servicio, inutilizando la disponibilidad de la información.	*Ejecutar la migración planeada para el 2018 con el fin de reemplazar los sistemas operativos obsoletos.	3	0,3	0,9
3. Falta de conocimiento para procesos de restauración a personal Backup del área encargada.	Software	Sistemas operativos obsoletos instalados y operativos en servidores productivos	Errores en la restauración del servicio y poca confiabilidad en la información almacenada.	*Capacitar a mínimo 2 empleados adicionales en la ejecución del proceso de restauración de Backups en la herramienta, con el fin de eliminar la dependencia de 1 solo empleado en momentos álgidos para la ejecución de dicho proceso.	2	0,2	0,4

3. Falta de conocimiento para procesos de restauración a personal Backup del área encargada.	Software	Pocas pruebas de intrusión para software operativo.	Software vulnerable a ataques informáticos que pueden poner en riesgo las operaciones de la organización.	*Capacitar a mínimo 2 empleados adicionales en la ejecución del proceso de restauración de Backups en la herramienta, con el fin de eliminar la dependencia de 1 solo empleado en momentos álgidos para la ejecución de dicho proceso.	2	0,2	0,4
3. Falta de conocimiento para procesos de restauración a personal Backup del área encargada.	Software	Caída del servicio	Errores al momento de restaurar información necesaria para las operaciones del negocio.	*Capacitar a mínimo 2 empleados adicionales en la ejecución del proceso de restauración de Backups en la herramienta, con el fin de eliminar la dependencia de 1 solo empleado en momentos álgidos para la ejecución de dicho proceso.	2	0,2	0,4
5. Falta de adiestramiento del personal para actuar en momento de crisis, no se hacen simulacros.	Software	Sistemas operativos obsoletos instalados y operativos en servidores productivos	Software desactualizado que conlleva a lentitud en las operaciones y posibles reprocesos al tener programas sin soporte que pueden fallar en cualquier momento.	*Verificar los simulacros y tiempos de respuesta en los ejercicios de simulación ejecutados, con el fin de mejorar en la medida de lo posible la reacción del personal involucrado.	2	0,3	0,6
5. Falta de adiestramiento del personal para actuar en momento de crisis, no se hacen simulacros.	Software	Pocas pruebas de intrusión para software operativo.	Software con falencias de seguridad que puede ser foco para ataques informáticos.	*Verificar los simulacros y tiempos de respuesta en los ejercicios de simulación ejecutados, con el fin de mejorar en la medida de lo posible la reacción del personal involucrado.	2	0,3	0,6
5. Falta de adiestramiento del personal para actuar en momento de crisis, no se hacen simulacros.	Software	Caída del servicio	Inoperatividad del servicio, inutilizando la disponibilidad de la información.	*Verificar los simulacros y tiempos de respuesta en los ejercicios de simulación ejecutados, con el fin de mejorar en la medida de lo posible la reacción del personal involucrado.	2	0,2	0,4
1. Versión de sistemas operativos obsoletos en servidores que se encuentran en operación.	Humanas	Falta de capacitación a personal Backup en el proceso de respaldo que puedan brindar apoyo al momento de ejecutar el proceso	Errores al momento de dar soporte/mantenimiento a los servicios cuando se requiera interactuar con servidores obsoletos.	*Ejecutar la migración planeada para el 2018 con el fin de reemplazar los sistemas operativos obsoletos.	3	0,3	0,9

3. Falta de conocimiento para procesos de restauración a personal Backup del área encargada.	Humanas	Falta de capacitación a personal Backup en el proceso de respaldo que puedan brindar apoyo al momento de ejecutar el proceso	Errores en el proceso de restauración de información.	*Capacitar a mínimo 2 empleados adicionales en la ejecución del proceso de restauración de Backups en la herramienta, con el fin de eliminar la dependencia de 1 solo empleado en momentos álgidos para la ejecución de dicho proceso.	2	0,2	0,4
3. Falta de conocimiento para procesos de restauración a personal Backup del área encargada.	Humanas	Documentación desactualizada de procesos.	Errores en el proceso de restauración de información.	*Capacitar a mínimo 2 empleados adicionales en la ejecución del proceso de restauración de Backups en la herramienta, con el fin de eliminar la dependencia de 1 solo empleado en momentos álgidos para la ejecución de dicho proceso.	2	0,2	0,4
5. Falta de adiestramiento del personal para actuar en momento de crisis, no se hacen simulacros.	Humanas	Documentación desactualizada de procesos.	Errores en el proceso de restauración de información.	*Verificar los simulacros y tiempos de respuesta en los ejercicios de simulación ejecutados, con el fin de mejorar en la medida de lo posible la reacción del personal involucrado.	2	0,2	0,4
9. Altos tiempos de respuesta del custodio de las cintas en sitios alternos de trabajo.	Humanas	Falta de capacitación a personal Backup en el proceso de respaldo que puedan brindar apoyo al momento de ejecutar el proceso	Confusión al momento de hacer restauración de la información debido a desconocimiento en el proceso de manejo de cintas.	*Definir de manera contractual con el proveedor multas y/o bonificaciones en caso de llegar tarde/rápido en momento de una eventualidad	1	0,3	0,3

Tabla 26 - Riesgo de residual